

Report Writer and Security Requirements Finder: User and Admin Manuals

Nancy R. Mead

CMU MSE Studio Team
Sankalp Anand
Anurag Gupta
Swati Priyam
Yaobin Wen
Walid El Baroni

June 2016

SPECIAL REPORT
CMU/SEI-2016-SR-002

CERT Division

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

<http://www.sei.cmu.edu>



Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg. 1305, 3rd floor
Hanscom AFB, MA 01731-2125

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

DM-0003414

Table of Contents

Abstract	iii
Report Writer User Manual	1
Report Writer Admin Guide	29
Security Requirements Finder User Manual	47
Security Requirements Finder Admin Guide	67

Abstract

This report presents instructions for using the Malware-driven Overlooked Requirements (MORE) website applications. The site enables requirements engineers and architects to bring the benefit of malware attack analysis to their own product development. They can examine reports of exploited vulnerabilities, frequently augmented by relevant misuse cases, use cases, and overlooked security requirements (MUO) that site contributors have posted. From this data they can search the site to identify security requirements suitable to their own projects. They can also contribute related content and new reports.

Users can interact with the site through two applications documented here. The Security Requirement Finder (SERF) allows site contributors to build on malware exploit reports, add MUOs while referencing Common Weakness Enumeration (CWE). The Report Writer application connects to SERF and aids contributors in adding MUOs to the exploit reports.

Instructions on performing these activities in both applications are presented here, as well as guides for performing admin tasks associated with the applications.

Report Writer User Manual

Report Writer User Manual

Table of Contents

Introduction	5
Roles	5
Public Users	5
Who is a public user?	5
What actions can you perform with Report Writer?	5
How will I access the Report Writer application?	5
How can I search for reports in the Report Writer application?	6
Report Writers.....	9
Who is a report writer?	9
I can view public reports. Can I write one of my own?	9
Okay, so how can I register?	9
Now that I have registered, can I log in?.....	12
So what must I do to be able to write a report?.....	13
How do I write a report now?	14
How will Report Writer provide suggestions?	15
Can I change the report contents after submission?.....	21
How will I know that my report has been accepted?	21
What else I can do as a report writer?	23
Reviewers	25
Who is a reviewer?	25
How can I become a reviewer?	25
What can I do as a reviewer?	25
Reports	25
Report rejection.....	25
Report publish/unpublish	26
CWE	27
Super User	27

Introduction

Report Writer and Security Requirement Finder (SERF) are applications through which users interact with the Malware-driven Overlooked Requirements (MORE) website. The MORE site presents a list of malware attack reports and the vulnerabilities that made those attacks possible. Such reports enable those who are building applications to learn of malware attacks others have undergone and the security requirements they can build into their projects to prevent such attacks. Report Writer is an application used by the exploit report writers that connects to SERF to help in adding misuse cases, use cases, and overlooked security requirements (MUO) to the exploit reports.

This user manual explains the activities that various users can perform in Report Writer and the steps they must take to complete them.

Roles

Three primary roles engage with the Report Writer application:

1. public user
2. report writer
3. reviewer

There is also one admin super user. The features accessible to each of these roles are described in this section.

Public Users

Who is a public user?

A public user is someone who is about to build an application, such as a requirements engineer or an architect. If you are such a user, you will want to be aware, before you start to build, of malware attacks your application might face. You can go to the Report Writer web application to read about malware attacks that others have reported.

What actions can you perform with Report Writer?

As of now, a public user can only search and view reports hosted in this system.

How will I access the Report Writer application?

Open a browser and type in the following URL: <http://report-writer.herokuapp.com/>

This will open the home page of the application, as shown in Figure 1. You will see a search bar in the lower half of this home page that you can use to search for reports.

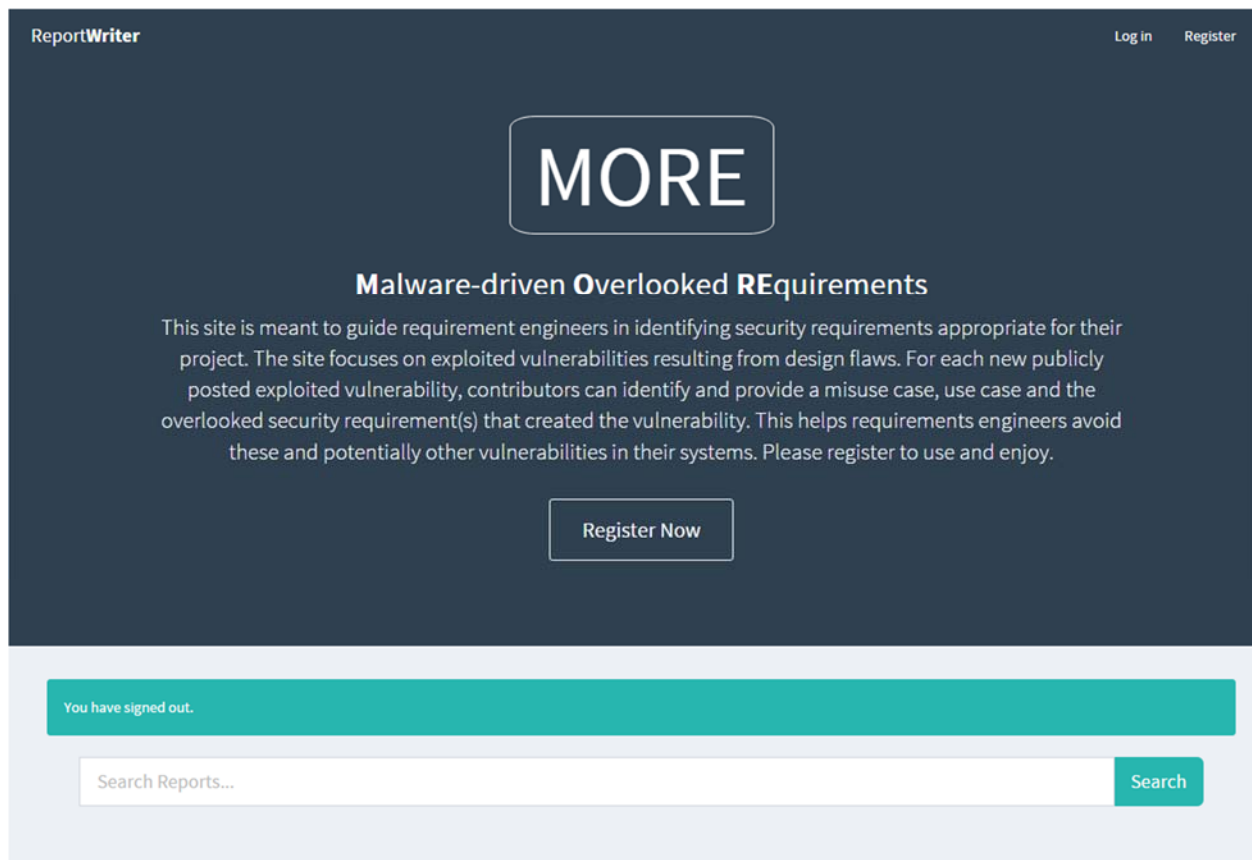


Figure 1

How can I search for reports in the Report Writer application?

There are two ways to search for reports:

- In the search bar, type in any text from the title of a specific report and search for the report matching the text.
- Browse through existing reports and select one or more that interests you.

Regarding the first method, let's say you came to know that PHPWiki was attacked by some kind of malware. You want more information on this particular attack, so you type PHPWiki in the search bar and click "Search". You will see the reports that match this search text. (See Figure 2.)

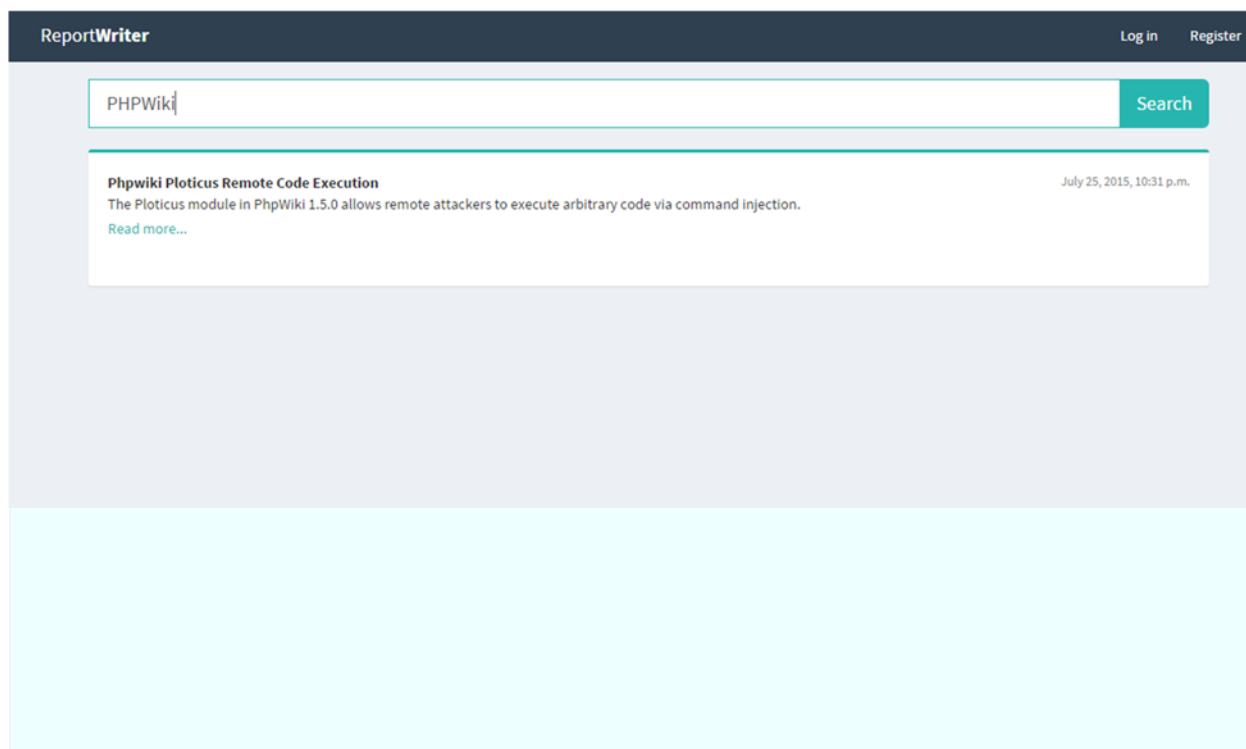


Figure 2

Regarding the second method, if you don't have the application name to search, you can simply scan through the reports and pick the one that interests you. Click "Search" without typing anything in the search field. The system will show you every report hosted in Report Writer. (See Figure 3.)

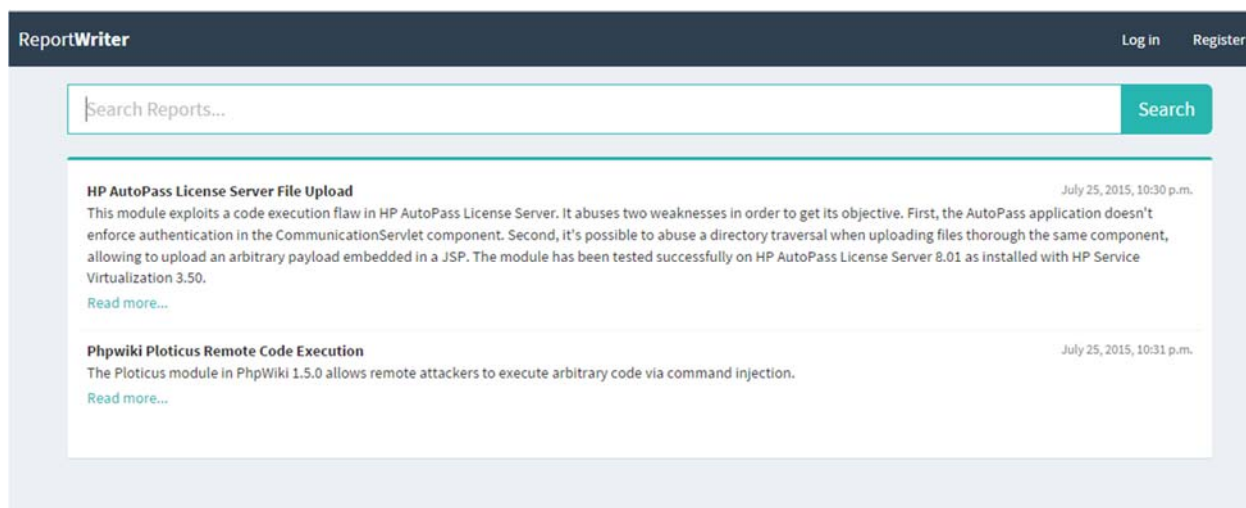


Figure 3

Next, you can open the file and read it. To do this, click on "Read more..." at the bottom of each report. The whole report opens. (See Figure 4.)

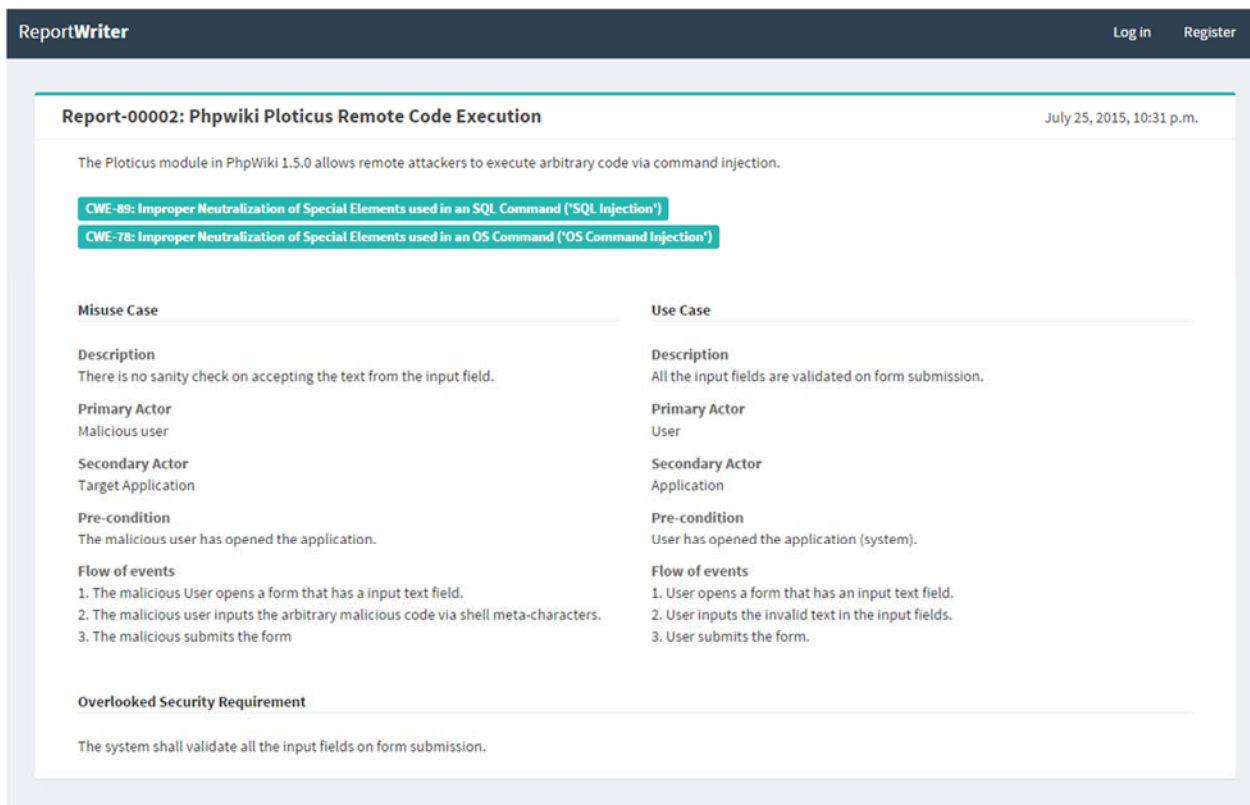


Figure 4

The application displays the following fields for a report.

1. Heading
2. Description
3. Common Weakness Enumerations (CWEs) and their IDs
4. Misuse Case
5. Use Case
6. Overlooked Security Requirements

Now we will explore the role of a report writer who creates these reports and makes them available to the public user.

Report Writers

Who is a report writer?

A report writer is someone who writes malware/exploit reports and contributes to the report repository.

I can view public reports. Can I write one of my own?

No. To write a report, you must be registered in the system. This operation mimics the behavior of Rapid 7 (<http://www.rapid7.com/db/>), wherein all public users can see all the reports hosted in the system, but only the authorized users can write the reports.

These reports also require approval from the reviewer, but we'll come to that when we talk about the reviewer role.

Okay, so how can I register?

It's simple. Open the application using the following URL: <http://report-writer.herokuapp.com/> Now click "Register" on top right corner. The following screen displays. (See Figure 5.)

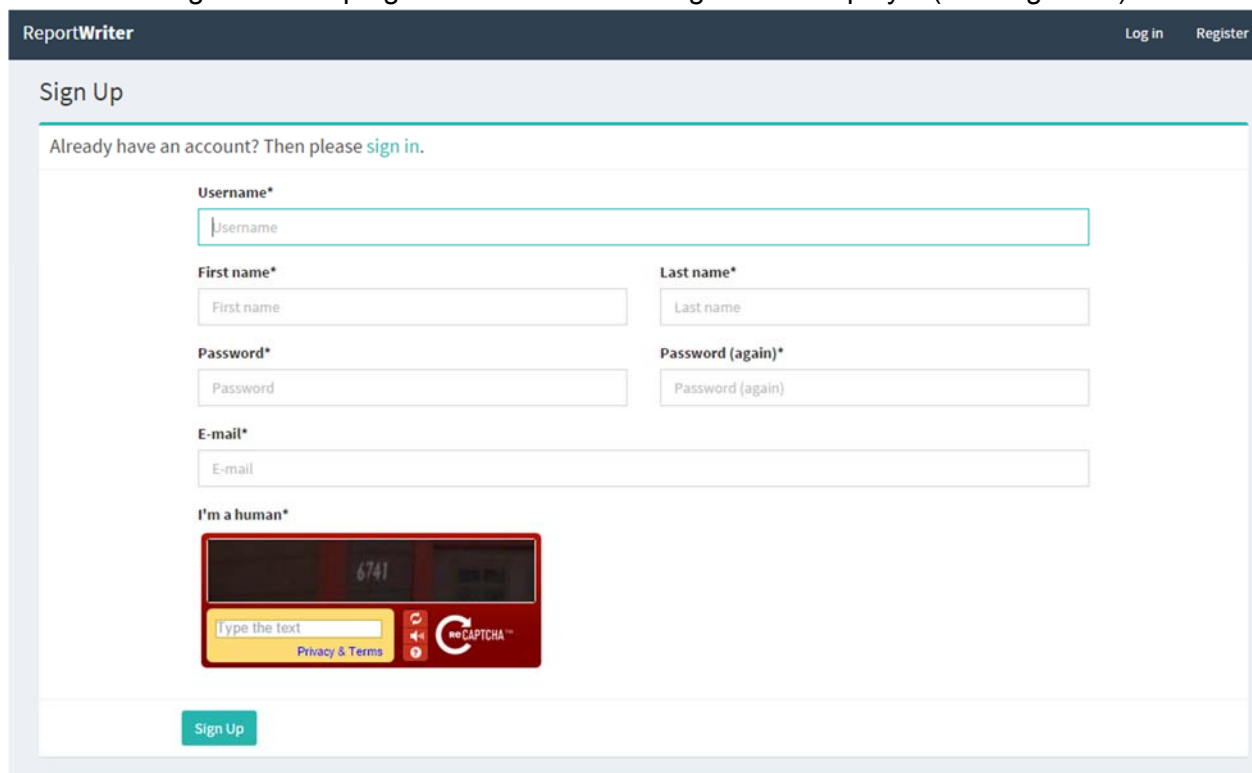
The image is a screenshot of a web application's registration page. At the top, a dark blue header bar contains the text "ReportWriter" on the left and "Log in" and "Register" on the right. Below the header, the page has a light blue background. A section titled "Sign Up" is centered. Below this title, a link says "Already have an account? Then please [sign in](#)." The registration form consists of several input fields: "Username*" (a single wide field), "First name*" and "Last name*" (two side-by-side fields), "Password*" and "Password (again)*" (two side-by-side fields), and "E-mail*" (a single wide field). Below these is a "I'm a human*" section featuring a CAPTCHA interface with a red border, a black display showing "6741", and a "noCAPTCHA" logo. At the bottom left of the form area is a green "Sign Up" button.

Figure 5

Fill in your details and click “Sign Up”. After you submit the form, the following screen displays. (See Figure 6.)

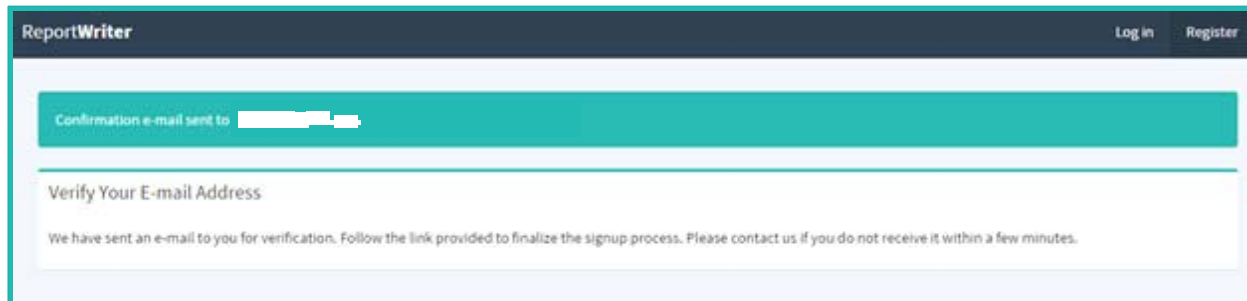


Figure 6

The next step is to go to your inbox and find an email from reportwritingapplication@gmail.com. An email displays as shown below. (See Figure 7.)

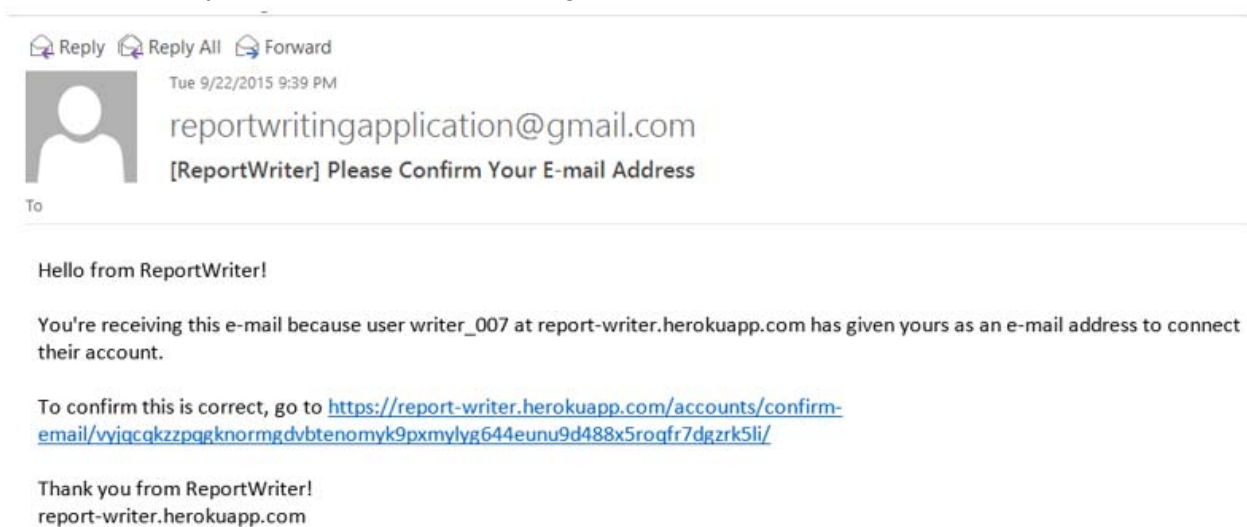


Figure 7

Click the link to confirm your email address. You return to the report writing application and the following page displays. (See Figure 8.)



Figure 8

Click “Confirm”. The following page displays. (See Figure 9.)

The image shows a web application interface with a light blue background. At the top, there is a teal banner with the text "You have confirmed janedoe@abc.org.". Below this is an orange banner with the text "Your registration request is pending for admin approval". The main content area is a white box with a light blue border. It contains the heading "Sign in to start your session". Below the heading are two input fields: "Username or e-mail" with an envelope icon and "Password" with a lock icon. There is a "Remember Me" checkbox and a "Sign In" button. At the bottom of the white box are two links: "I forgot my password" and "Register a new account".

You have confirmed janedoe@abc.org.

Your registration request is pending for admin approval

Sign in to start your session

Username or e-mail

Password

☐ Remember Me

Sign In

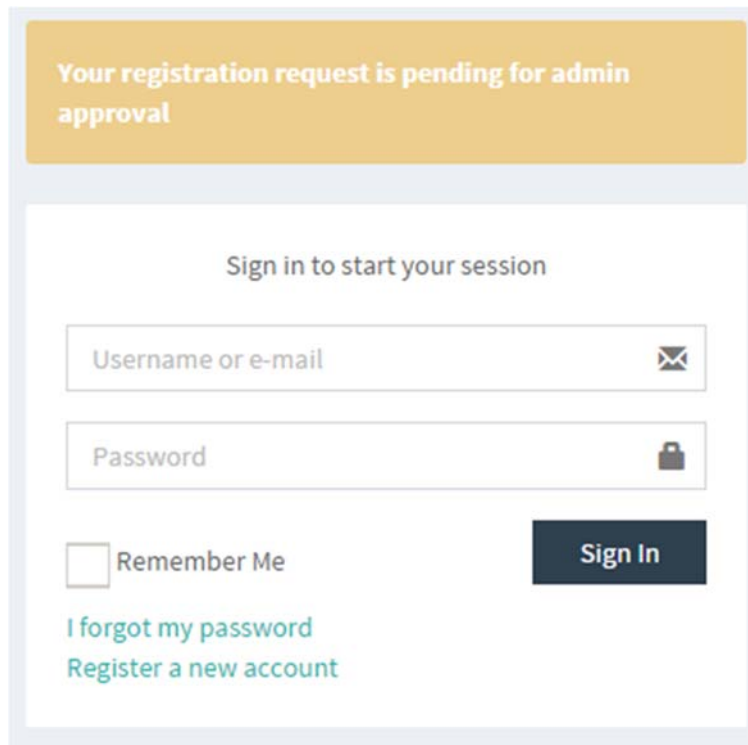
[I forgot my password](#)

[Register a new account](#)

Figure 9

Now that I have registered, can I log in?

Unfortunately not. There is an extra level of authentication in this application to prevent any arbitrary user from writing the report. If you try to log in, you will see an error message. (See Figure 10.)



Your registration request is pending for admin approval

Sign in to start your session

Username or e-mail

Password

☐ Remember Me

Sign In

[I forgot my password](#)

[Register a new account](#)

Figure 10

So what must I do to be able to write a report?

You must now wait until the reviewer receives this message and approves your request. (We'll show you how the reviewer accepts this request when we discuss the reviewer role in the next section. For now, just assume that the reviewer has accepted your request.) As soon as the reviewer accepts your request, you will receive an email as shown below (See Figure 11.)

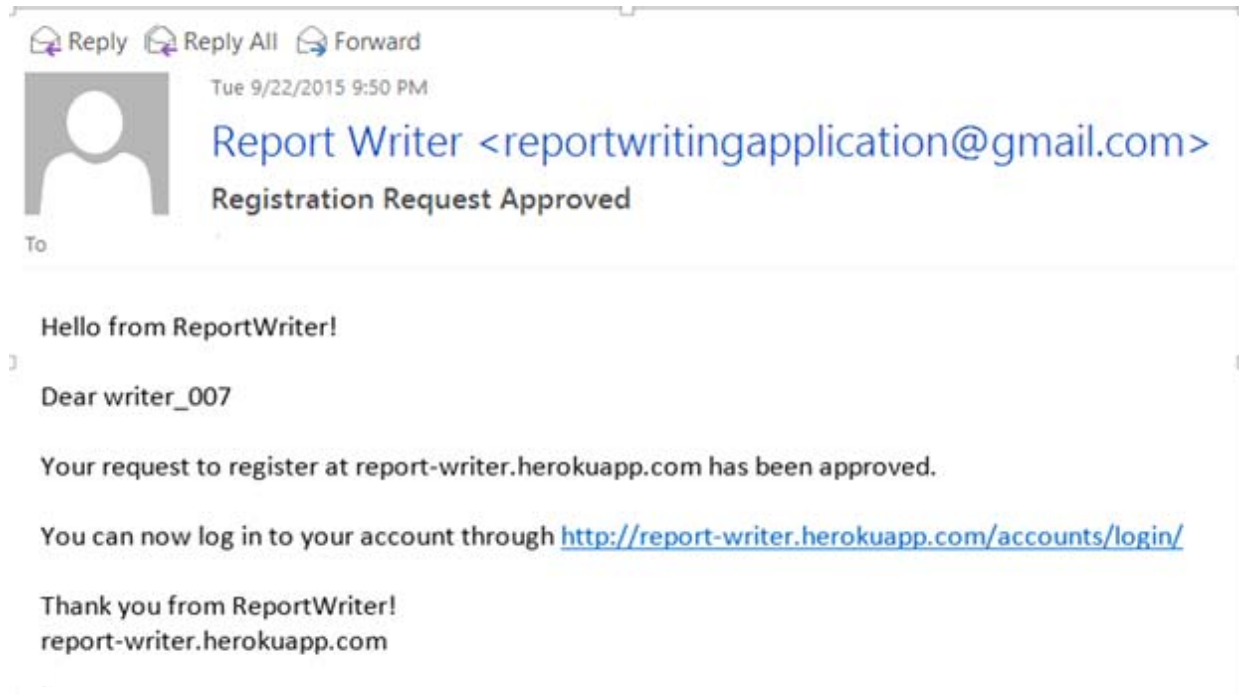


Figure 11

When you receive the email approval, log in using your credentials. The dashboard screen displays. (See Figure 12.)

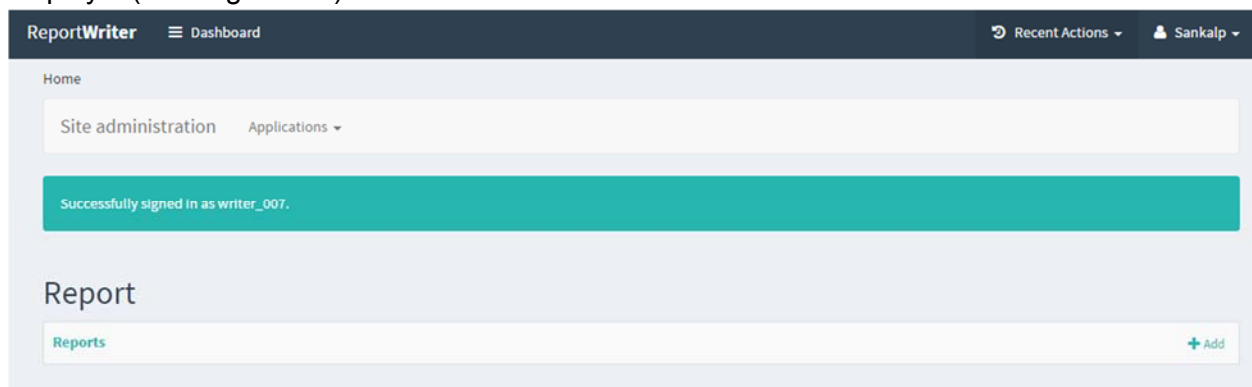


Figure 12

How do I write a report now?

Your dashboard shows all the features of the application available to you as a report writer. As of now, you have access to just one resource—reports. (If you have higher access in this application, you will see more resources/action items on your dashboard.)

From here you can either

- see how many approved reports are there in the system by clicking “Reports” in the above screen or
 - directly add a new report by clicking the “Add” button on the right
1. To view approved reports, Click “Reports”. The list of reports displays.
 2. From this list of all approved reports, you can click on any report to view it. The reports with all the details display as shown in the public user view.
 3. Click on the green button above “Add Report”.
 4. A page opens where you can create your reports. (See Figure 13.)

The screenshot shows the 'Add Report' form in the ReportWriter application. The header bar includes the 'ReportWriter' logo, a 'Dashboard' menu, and user information 'Recent Actions' and 'Sankalp'. The breadcrumb trail is 'Home / Report / Reports / Add Report'. The form itself has a title 'Add Report' and a 'Name' field with a slash '/' inside. To the right of the 'Name' field is a 'Status' dropdown menu currently set to 'Draft'. Below these is a 'Title*' text field. Underneath the title is a large 'Description*' text area. At the bottom of the form is a 'CWEs*' section with a text input field containing the instruction 'Either click 'Suggest CWEs' to get the suggest CWE based on your description or select a CWE from the list'. To the right of this field is a green 'Suggest CWEs' button. Below the 'CWEs*' section are two blue buttons: 'Write my own Misuse Case and Use Case' and 'Suggest Misuse Cases and Use Cases'. At the very bottom of the form are two buttons: 'Save and continue editing' and 'Save'.

Figure 13

You can also arrive at this page by clicking the “Add” button from the report list screen. Do this if you want to add a new report without first viewing the list of all approved reports.

How will Report Writer provide suggestions?

ReportWriter Dashboard Recent Actions Sankalp

Home / Report / Reports / Add Report

Add Report

Name / Status Draft

Title* Symantec Endpoint Protection Manager Authentication Bypass and Code Execution

Description* This module exploits three separate vulnerabilities in Symantec Endpoint Protection Manager in order to achieve a remote shell on the box as NT AUTHORITY\SYSTEM. The vulnerabilities include an authentication bypass, a directory traversal and a privilege escalation to get privileged code execution.

CWEs* Either click "Suggest CWEs" to get the suggest CWE based on your description or select a CWE from the list Suggest CWEs

Write my own Misuse Case and Use Case Suggest Misuse Cases and Use Cases

Save and continue editing Save

Figure 14

Click “Suggest CWEs”. The system will pull up suggestions by parsing your text. The suggestions appear as shown on the next page. (See Figure 15.)

* REST stands for Representational State Transfer. REST is an architecture style for designing networked applications. It relies on a stateless, client-server, cacheable communications protocol—and in virtually all cases, the HTTP protocol is used. REST API allows for seamless integration of functionality between applications.

Elkstein, M., 2008. “Learn REST: A Tutorial.” <http://rest.elkstein.org/2008/02/what-is-rest.html>

ReportWriter Dashboard Recent Actions Sankalp

Home / Report / Reports / Add Report

Add Report

Name: / Status: Draft

Title*: Symantec Endpoint Protection Manager Authentication Bypass and Code Execution

Description*: This module exploits three separate vulnerabilities in Symantec Endpoint Protection Manager in order to achieve a remote shell on the box as NT AUTHORITY\SYSTEM. The vulnerabilities include an authentication bypass, a directory traversal and a privilege escalation to get privileged code execution.

CWEs*:

- × CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key
- × CWE-535: Information Exposure Through Shell Error Message
- × CWE-639: Authorization Bypass Through User-Controlled Key
- × CWE-603: Use of Client-Side Authentication
- × CWE-305: Authentication Bypass by Primary Weakness
- × CWE-494: Download of Code Without Integrity Check
- × CWE-650: Trusting HTTP Permission Methods on the Server Side
- × CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote
- × CWE-385: Covert Timing Channel
- × CWE-408: Incorrect Behavior Order: Early Amplification

[Suggest CWEs](#)

[Write my own Misuse Case and Use Case](#) [Suggest Misuse Cases and Use Cases](#)

[Save and continue editing](#) [Save](#)

Figure 15

You can delete the CWE suggestions not relevant to you. You can even add new ones by typing in the CWEs box; y Additional suggestions will appear. (See Figure 16.)

Description*: This module exploits three separate vulnerabilities in Symantec Endpoint Protection Manager in order to achieve a remote shell on the box as NT AUTHORITY\SYSTEM. The vulnerabilities include an authentication bypass, a directory traversal and a privilege escalation to get privileged code execution.

CWE-301: Reflection Attack in an Authentication Protocol

CWE-302: Authentication Bypass by Assumed-Immutable Data

CWE-304: Missing Critical Step in Authentication

CWE-306: Missing Authentication for Critical Function

CWE-307: Improper Restriction of Excessive Authentication Attempts

CWE-308: Use of Single-factor Authentication

CWEs*:

- × CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key
- × CWE-535: Information Exposure Through Shell Error Message
- × CWE-639: Authorization Bypass Through User-Controlled Key
- × CWE-603: Use of Client-Side Authentication
- × CWE-305: Authentication Bypass by Primary Weakness
- × CWE-494: Download of Code Without Integrity Check
- × CWE-650: Trusting HTTP Permission Methods on the Server Side
- × CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote
- × CWE-385: Covert Timing Channel
- × CWE-408: Incorrect Behavior Order: Early Amplification

[Suggest CWEs](#)

Figure 16

When you have finished selecting the CWE suggestions, you have two options. You can either

- request suggestions for misuse cases and use cases or
- write one of your own

To take the first option, click on “Suggest Misuse Cases and Use Cases”. The suggested misuse case appears in a Mac-Finder-like view. (See Figure 17.)

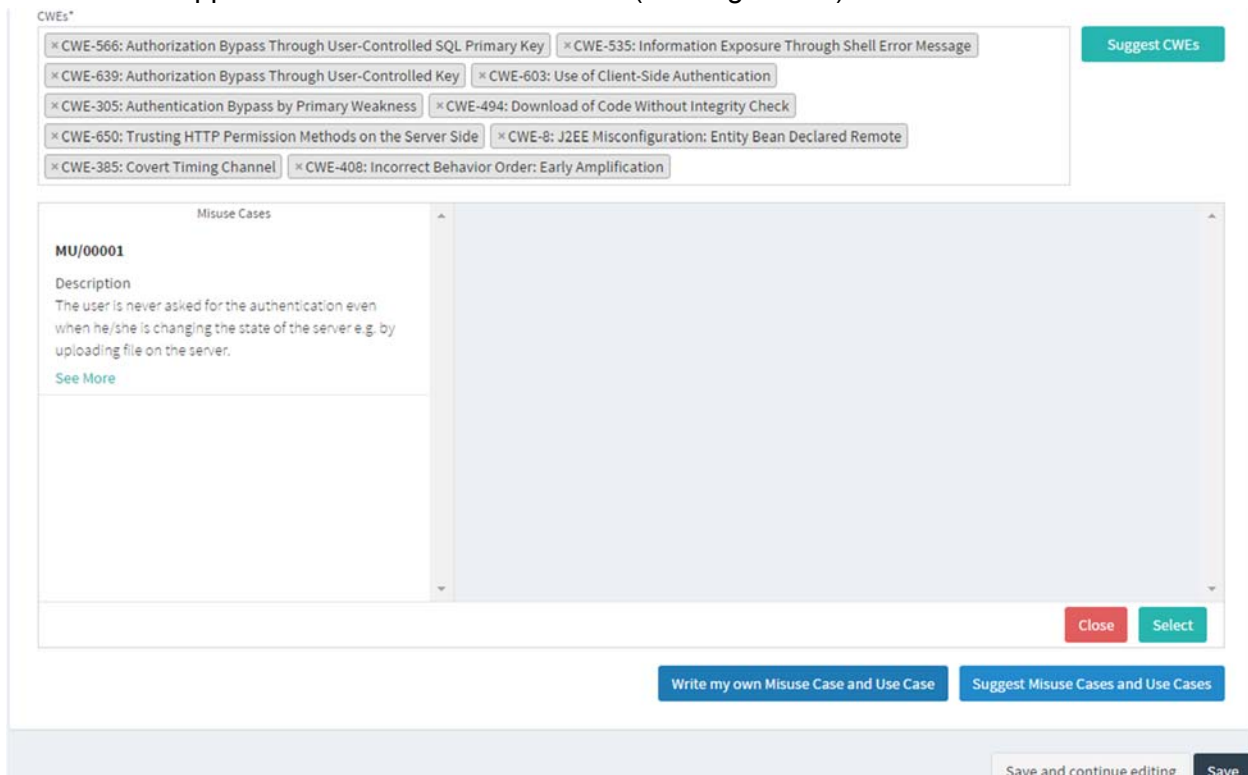


Figure 17

Currently one misuse case appears for the selected CWE. To select any misuse case, click it in the left panel. The right panel populates with the use case and overlooked security requirements. (See Figure 18.) Select one of these.

CWEs*

CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key
CWE-535: Information Exposure Through Shell Error Message

CWE-639: Authorization Bypass Through User-Controlled Key
CWE-603: Use of Client-Side Authentication

CWE-305: Authentication Bypass by Primary Weakness
CWE-494: Download of Code Without Integrity Check

CWE-650: Trusting HTTP Permission Methods on the Server Side
CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote

CWE-385: Covert Timing Channel
CWE-408: Incorrect Behavior Order: Early Amplification

Suggest CWEs

Misuse Cases

MU/00001

Description
The user is never asked for the authentication even when he/she is changing the state of the server e.g. by uploading file on the server.

See More

Use Cases & Overlooked Security Requirements

Use Case: UC/00001

Description
The user is asked for the authentication when he/she is changing the state of the server e.g. by uploading file on the server.

Primary Actor
User

Secondary Actor
Application

Pre-condition
User has opened the application (system).

Close

Select

Write my own Misuse Case and Use Case

Suggest Misuse Cases and Use Cases

Save and continue editing

Save

Figure 18

After selecting, you can save the report by first clicking on “Select” and then on “Save”. The text areas for report details will be auto populated for the selected Misuse Case and Use case. (See Figure 19.)

CWEs*

CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key
CWE-535: Information Exposure Through Shell Error Message

CWE-639: Authorization Bypass Through User-Controlled Key
CWE-603: Use of Client-Side Authentication

CWE-305: Authentication Bypass by Primary Weakness
CWE-494: Download of Code Without Integrity Check

CWE-650: Trusting HTTP Permission Methods on the Server Side
CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote

CWE-385: Covert Timing Channel
CWE-408: Incorrect Behavior Order: Early Amplification

Suggest CWEs

Write my own Misuse Case and Use Case

Suggest Misuse Cases and Use Cases

Misuse Case:

Description

The user is never asked for the authentication even when he/she is changing the state of the server e.g. by uploading file on the server.

Primary actor

Malicious user

Secondary actor

Target Application

Pre-condition

Malicious user has opened the application (system) and has the malicious/harmful file to be uploaded onto the server.

Flow of events

Use Case:

Description

The user is asked for the authentication when he/she is changing the state of the server e.g. by uploading file on the server.

Primary actor

User

Secondary actor

Application

Pre-condition

User has opened the application (system).

Flow of events

Figure 19

If you are not satisfied with the suggested misuse case, you can choose to write one of your own. Click “Write my own Misuse Case and Use Case”. Additional text areas appear for you to fill in to complete the report. (See Figure 20.)

Write my own Misuse Case and Use Case Suggest Misuse Cases and Use Cases

Misuse Case:

Description

Primary actor

Secondary actor

Pre-condition

Flow of events

Post-condition

Assumption

Source

Use Case:

Description

Primary actor

Secondary actor

Pre-condition

Flow of events

Post-condition

Assumption

Source

Figure 20

After completing the fields, click “Save” to save the report as a draft. The previous list of reports screen appears. (See Figure 21.)

Home / Report / Reports


Select Report to change [+ Add Report](#)

<input type="checkbox"/>	Name	Status
<input type="checkbox"/>	Report-00004	Draft
<input type="checkbox"/>	Report-00003	Approved
<input type="checkbox"/>	Report-00001	Approved

Action: 0 of 3 selected

Figure 21

To submit the draft report, reopen it and click “Submit for Review” at the bottom of the screen.

A horizontal bar containing three buttons: a red 'Delete' button on the left, a light blue 'Submit for Review' button in the center, and a dark blue 'Save' button on the right. A 'Save and continue editing' button is also visible between 'Submit for Review' and 'Save'.

Your report will be saved, and all the fields will become read-only. The report is now awaiting approval by the reviewer. The status for this report in the report list screen will be “In Review”.

A screenshot of a report list table with columns for Name and Status. It shows three reports: Report-00004 (In Review), Report-00003 (Approved), and Report-00001 (Approved). Below the table is an action bar with a dropdown menu, a 'Go' button, and a selection count '0 of 3 selected'.

Figure 22

Can I change the report contents after submission?

You can, but only before it is approved. First go to the bottom of the report and click “Reopen”. Your report reopens and you can make your changes and save the report just as you saved it the first time. (See Figure 23.)

Once the report is approved, you cannot perform further action on it.

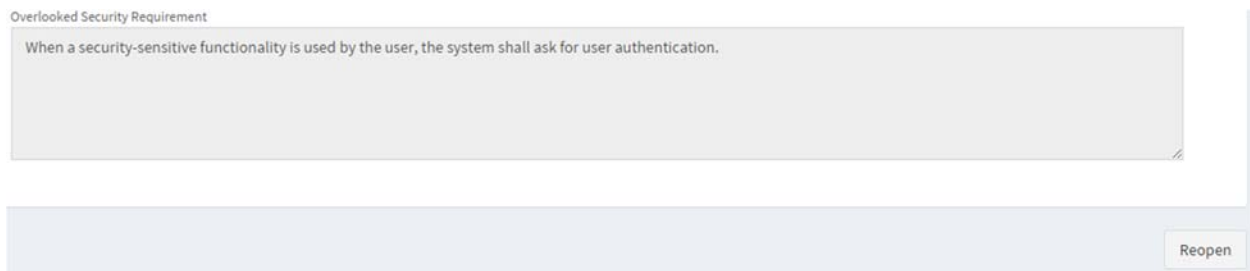
A screenshot showing a report content area with the title 'Overlooked Security Requirement' and a description 'When a security-sensitive functionality is used by the user, the system shall ask for user authentication.' Below this is a large light blue bar with a 'Reopen' button on the right side.

Figure 23

How will I know that my report has been accepted?

You will receive an email notifying you of your report’s acceptance. (See Figure 24.) Its status will change to “Approved” in the report list screen.

 Reply  Reply All  Forward



Tue 9/22/2015 10:50 PM

Report Writer <reportwritingapplication@gmail.com>

Your Report has been accepted

To

Dear!

Your Report Report-00003 has been accepted

You have been notified because you set yourself as a listener for this activity.
To make changes, please edit your preferences

- Report Writing Application

Figure 24

What else I can do as a report writer?

You can view and change your profile. To do this, click your name in the top right corner and then click “My Profile”. (See Figure 25.)

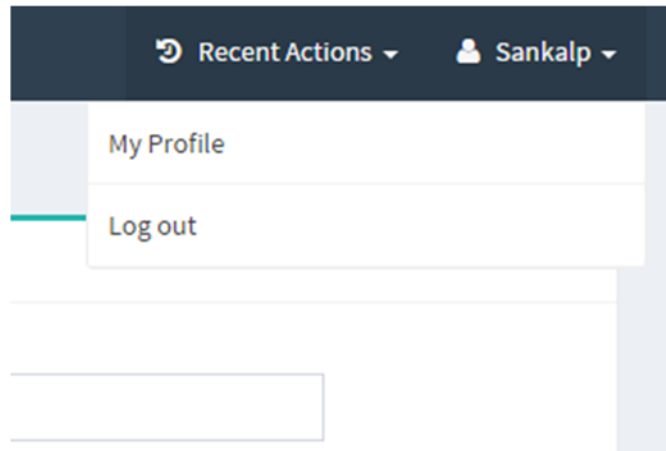


Figure 25

The update profile page displays.

Here you can do the following:

1. Change your display name.
2. Change your password.
3. Change your email preferences.
4. Change your notification settings.
5. Deactivate your account.

(See Figure 26.)

The screenshot shows a 'My Profile' page with two main sections. The 'Personal Information' section contains input fields for 'First name' (Jane) and 'Last name' (Doe). Below these fields are links for 'Change My Password' and 'Manage My Emails'. The 'Notification Settings' section has three checkboxes, all of which are checked: 'When My Report is Accepted', 'When My Report is Rejected', and 'When My Report is Commented On'. At the bottom of the page, there is a red button labeled 'Deactivate My Account' and a green 'Save' button in the bottom right corner.

Figure 26

If you click “Manage My Emails”, you’ll be presented with options to add another email to this account, remove the existing one, make an email primary, and resend verification link. (See Figure 27.)

The screenshot shows an 'E-mail Addresses' page. It starts with the heading 'E-mail Addresses' and a message: 'The following e-mail addresses are associated with your account:'. Below this, there is a list of email addresses. The first one is 'janedoe@abc.org', which is marked as 'Verified' (green button) and 'Primary' (blue button). Below the email address are three buttons: 'Make Primary' (dark blue), 'Re-send Verification' (dark blue), and 'Remove' (red). Below this list, there is a section titled 'Add E-mail Address' with a label 'E-mail*' and an empty input field. At the bottom of this section is a dark blue button labeled 'Add E-mail'.

Figure 27

Reviewers

Who is a reviewer?

A reviewer is someone who approves the reports so that they can be made available to the public.

How can I become a reviewer?

You must register in the same manner as a report writer. The super user will determine if you can escalate to the reviewer access level.

What can I do as a reviewer?

As a reviewer, you can add/edit/view CWEs, view issues raised for some reports, and approve the reports. You'll find each activity explained below.

Reports

If you click Reports, the list of all the approved reports in the system will display. Additionally, you will see which reports are awaiting review.

<input type="checkbox"/>	Name	Status
<input type="checkbox"/>	Report-00004	In Review
<input type="checkbox"/>	Report-00003	Approved
<input type="checkbox"/>	Report-00001	Approved

To approve a report, open an In Review report. At the bottom of the report screen, click the “Approve” button. The report is approved with the following notification.

You have approved the submission

Name	Status
Report-00004	Approved

Figure 28

Report rejection

You can reject or unpublish any report. You might choose to do so when it is a duplicate of another report, is incorrect, or uses offensive language. To reject a report, open it and click on the “Reject” button. A pop-up will appear.

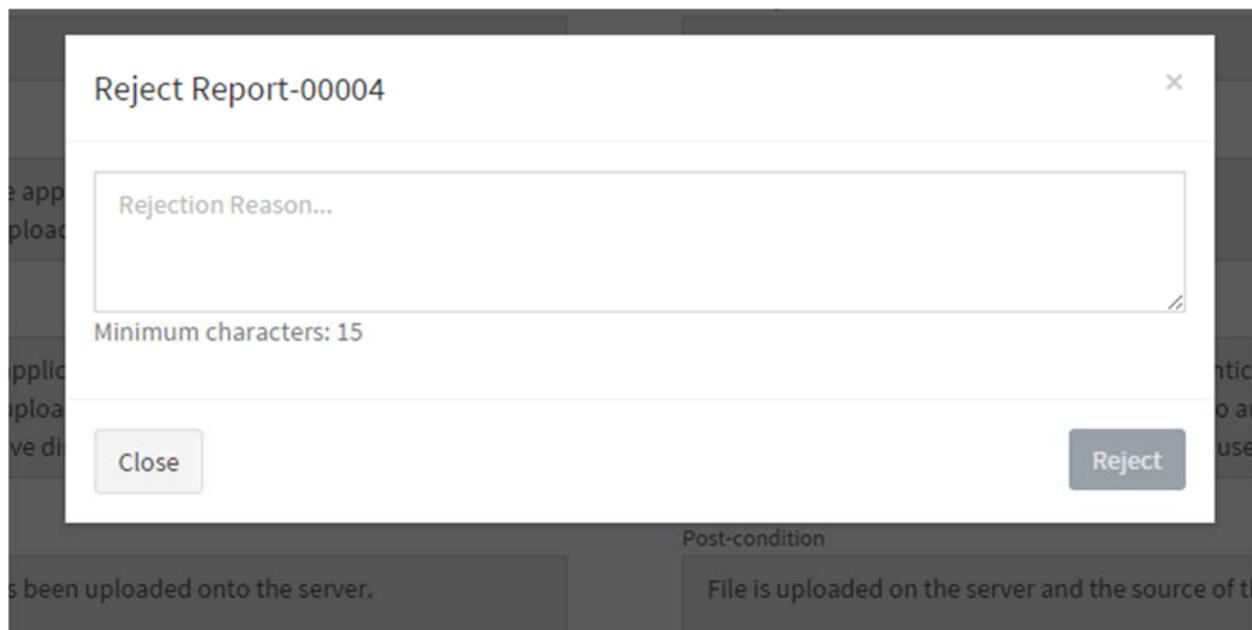


Figure 29

In the pop-up, type in the reason for rejection and click “Reject”. The report is rejected and a message is sent to the author. The author can still reopen the report and re-submit it by making required changes that you prescribed.



Figure 30

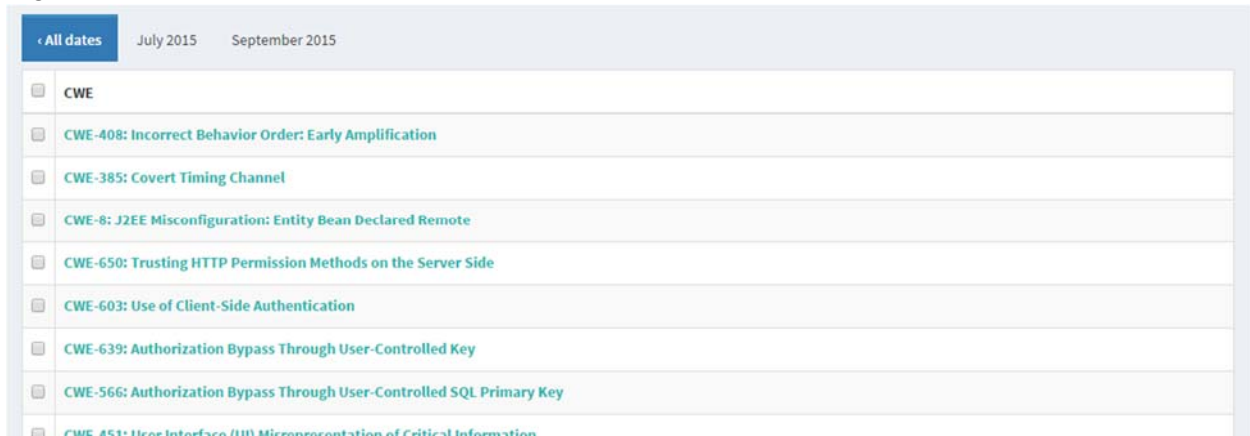
Report publish/unpublish

There is an additional button on every approved report. It is called “Unpublish”. You may want to take a report offline for some reason. For example, you may learn that it contains errors or offensive language or is a duplicate, but still slipped through to publication. In such cases you would unpublish the report.

Once the MUO is unpublished, you can either publish it back or republish it. You can republish it with or without making changes. If you have unpublished it in error, you can publish it back as it is.

CWE

The Report Writer has a list of CWEs so that it can associate its reports with the CWEs. You can access those CWEs here. Click on CWEs. A list of CWEs in the system displays. (See Figure 31.)

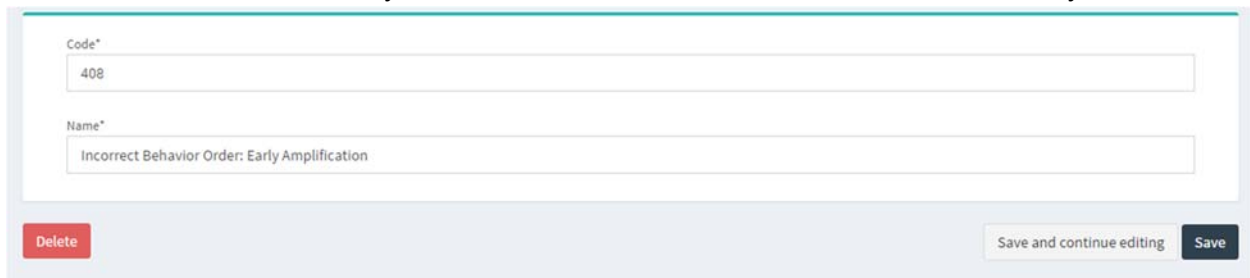


The screenshot shows a web interface for managing CWEs. At the top, there are tabs for 'All dates', 'July 2015', and 'September 2015'. Below the tabs is a table with the following rows:

<input type="checkbox"/>	CWE
<input type="checkbox"/>	CWE-408: Incorrect Behavior Order: Early Amplification
<input type="checkbox"/>	CWE-385: Covert Timing Channel
<input type="checkbox"/>	CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote
<input type="checkbox"/>	CWE-650: Trusting HTTP Permission Methods on the Server Side
<input type="checkbox"/>	CWE-603: Use of Client-Side Authentication
<input type="checkbox"/>	CWE-639: Authorization Bypass Through User-Controlled Key
<input type="checkbox"/>	CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key
<input type="checkbox"/>	CWE-451: User Interface (UI) Misrepresentation of Critical Information

Figure 31

You can click the name of any CWE to edit it. You can also add new ones to the system.



The screenshot shows a form for editing a CWE. It has two input fields: 'Code*' with the value '408' and 'Name*' with the value 'Incorrect Behavior Order: Early Amplification'. At the bottom, there are three buttons: 'Delete' (red), 'Save and continue editing' (light blue), and 'Save' (dark blue).

Figure 32

Super User

A super user is someone who has the highest level of access in the application. (See Figure 33.)

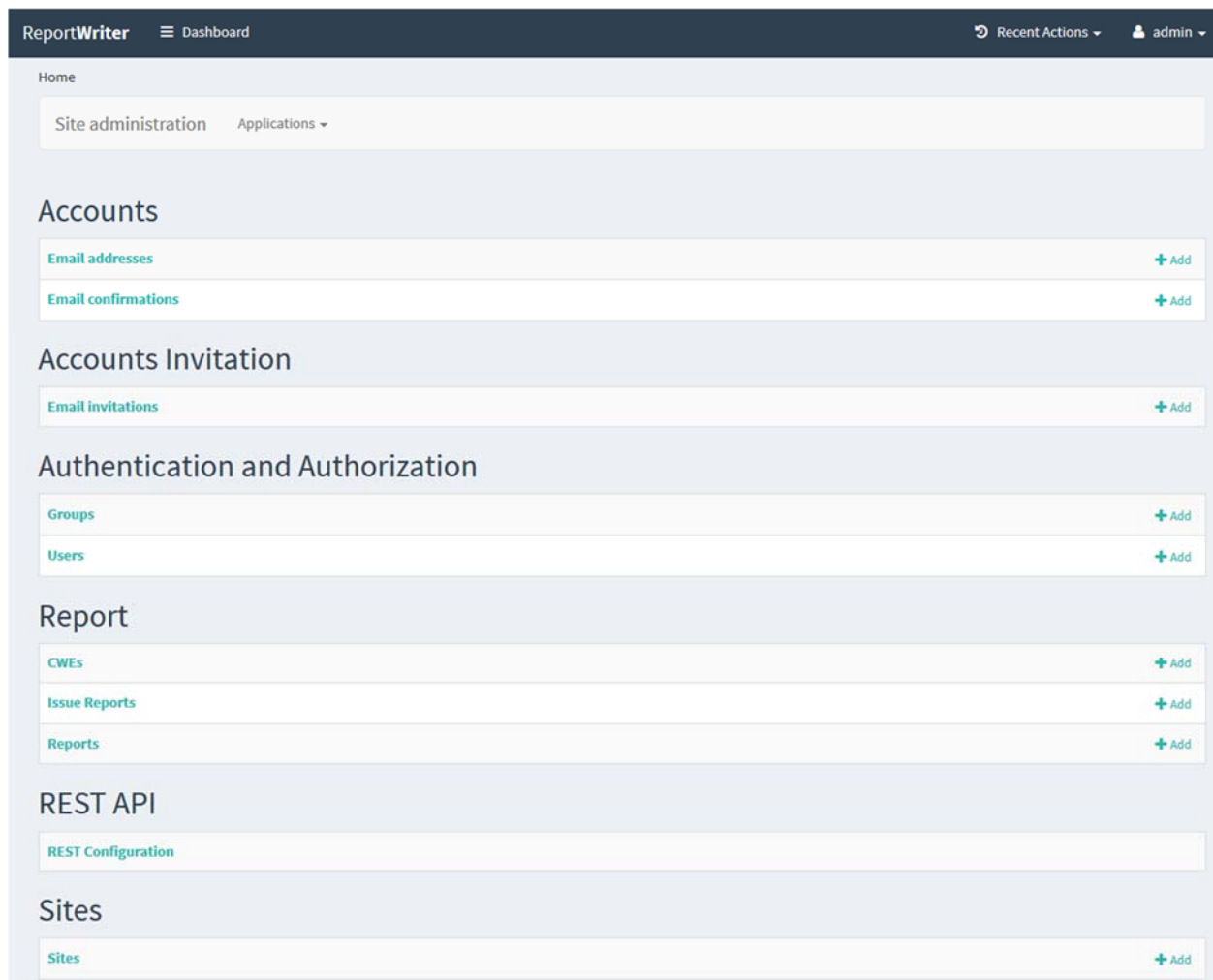


Figure 33

The only difference between the super user and the admin is that the admin role is created by the super user. In the REST API, the admin will be able to save the SERF (REST API) URL. The admin can also set the Token on this same screen. (See Figure 34.) This token is used for authenticating Report Writer with the MORE application. Without this token, the Report Writer application wouldn't be able to consume the web service. Note that this is just one set of the REST API settings. You can only edit it; you cannot add new ones.

The screenshot shows a form for configuring the REST API. It has two input fields: 'Url*' with the value 'https://enhanced-cwe.herokuapp.com/api/v1' and 'Token*' with the value 'd9cdcc1ee2902c1f18254367d15a79562d0a31f2'. At the bottom right, there are two buttons: 'Save and continue editing' and 'Save'.

Figure 34

Report Writer Admin Guide

Report Writer Admin Guide

Table of Contents

Introduction	33
Intended Audience	33
Common Scenarios	33
Pages	33
Home page	33
Dashboard Page	34
Common Administration Operations	35
Add	36
Modify	36
Delete	37
Save	39
Tasks	39
Log in	39
Log out	40
Approve New User's Registration	41
Privilege Management	43
Group Management	43
User Management	44
REST API Management	46

Introduction

This document is the admin guide for the web-based Report Writer application. It describes the detailed steps the application admin must follow to accomplish application and user-management tasks.

The document is divided into two major sections:

1. **Common Scenarios:** This section describes the frequently mentioned pages and common operations that can be shared by all the tasks, such as how to add, change or delete an item.
2. **Tasks:** This section describes the detailed steps for accomplishing the application and user management tasks that the application admin may need to perform, such as how to approve a user's registration.

Intended Audience

This document is intended for the admin of the Report Writer application.

Common Scenarios

Throughout the document, certain concepts and web pages are mentioned frequently. They are listed and defined in this section.

Pages

Home page

The home page is the first page users see when they enter the website URL. It displays the title and a brief introduction to the website. (See Figure 1.)

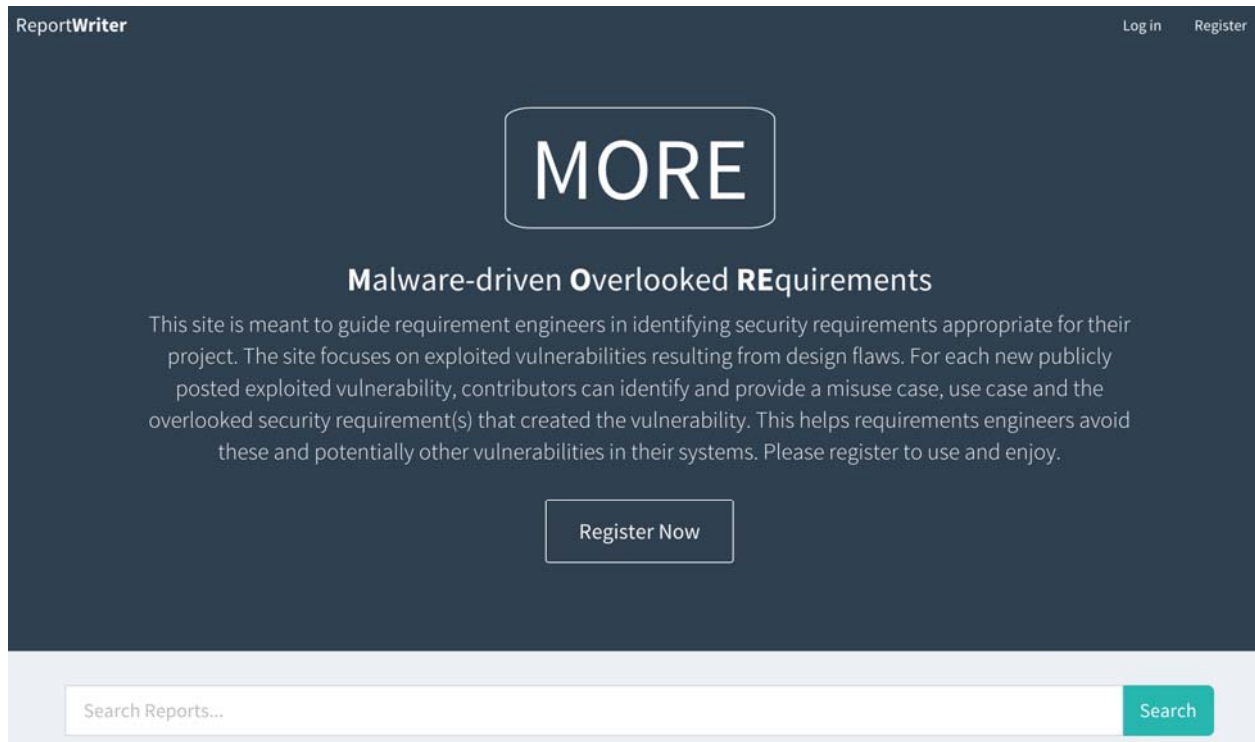


Figure 1: Home page

Dashboard Page

After you log in, the dashboard page appears, which lists all manageable items. (See Figure 2.)

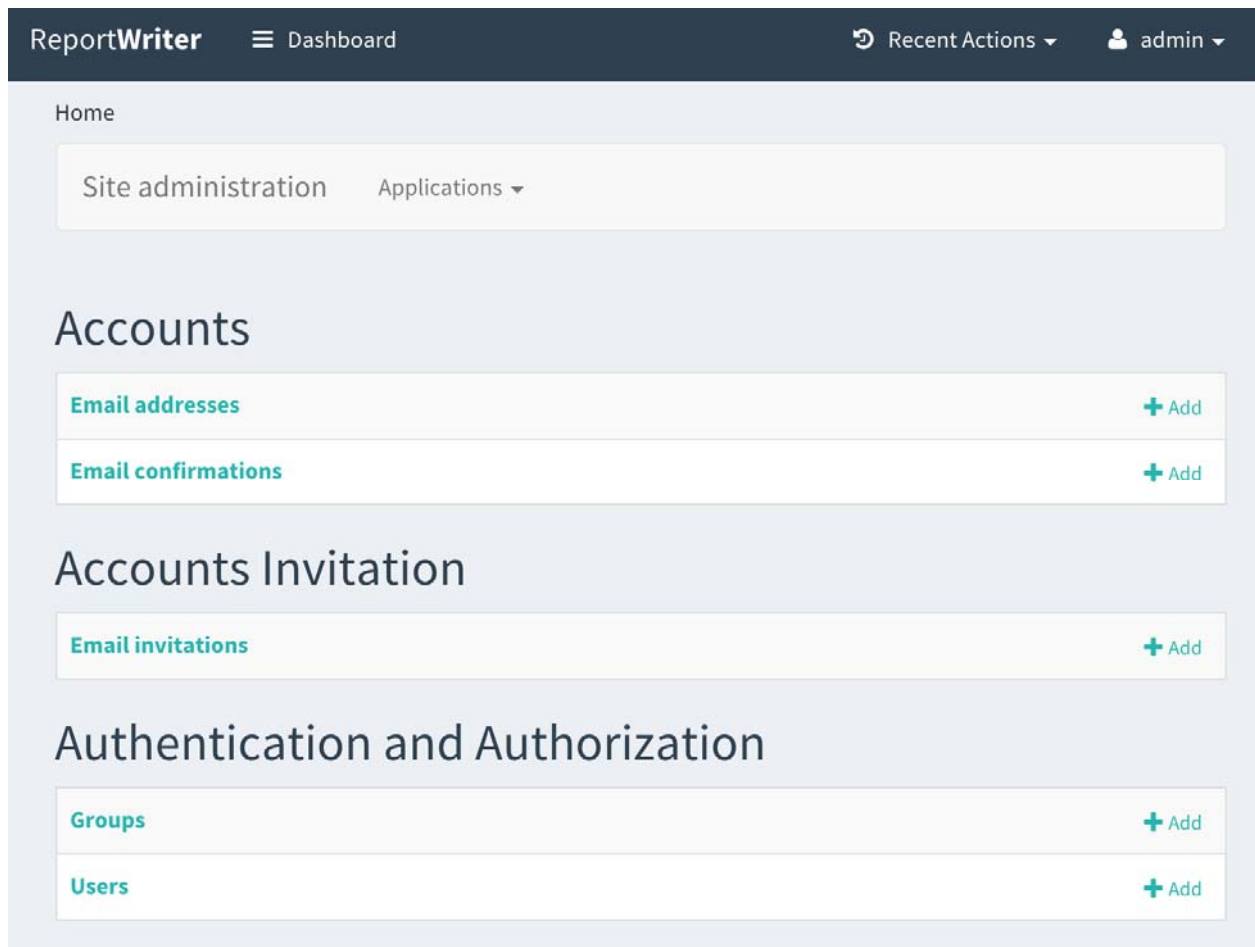


Figure 2: Dashboard Page (partial view)

Common Administration Operations

The Report Writer website is created with a consistent look and feel for management operations, so the management of different functions looks very similar. Each function is explained below.

The typical management operations include the following:

- **Add:** Add a new instance, such as a user group.
- **Save:** Save the current modification.
- **Modify:** Modify the information of an existing instance.
- **Delete:** Delete an existing instance.

As an example, the management of user groups will serve to show how to perform addition, modification, or deletion in the website. Beyond user groups, the four operations above can be applied to other managed entities, including the following:

- email addresses, email confirmations, and email invitations
- groups and users

- CWEs, issue reports, and reports
- sites
- user profiles

Add

You can add a user group in one of two ways: through “Add” in the dashboard page or the “Add” button in the group list page.

In the dashboard page, locate “Groups” in the “Authentication and Authorization” section. There is a “+Add” button on the right-hand side. Click it to open the group adding page.

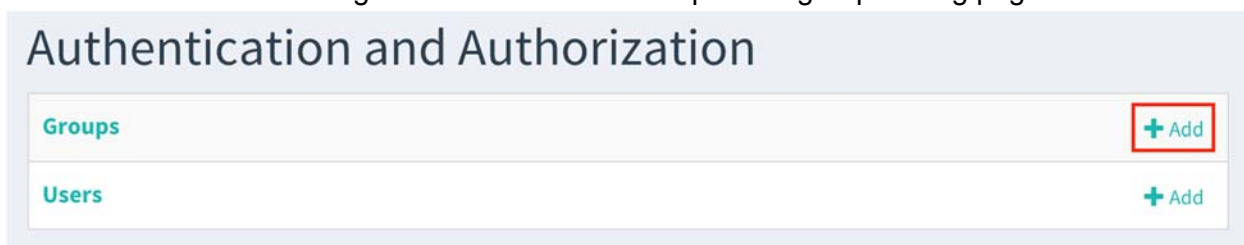


Figure 3: Add a group

Alternatively, you can click the “Groups” name first to open the group list page, then click the “Add group” button to open the group adding page. (See Figure 4 and Figure 5.)

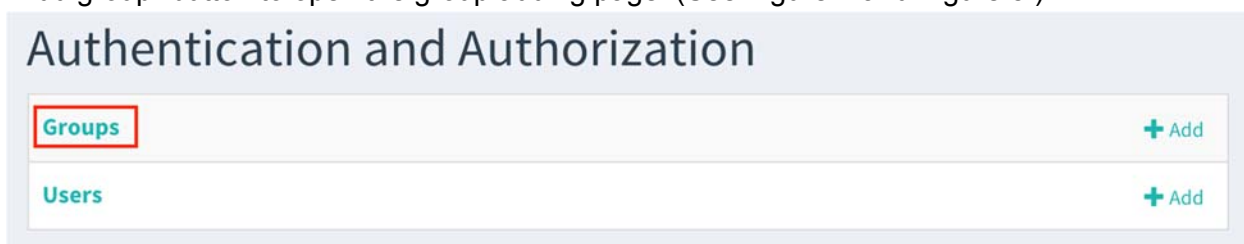


Figure 4: Click “Groups”

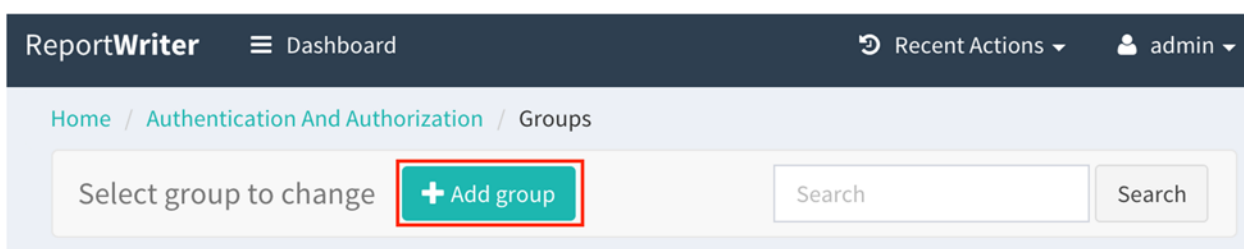


Figure 5: Click “Add group” to open the group adding page

Modify

To modify a group’s settings, follow the steps below:

1. In the dashboard page, navigate to the group list page through “Authentication and Authorization” -> “Groups”. (See Figure 4 above.)

2. In the group list, click the name of the group for which information is to be changed. The Change group page opens. (See Figure 6 and Figure 7.)

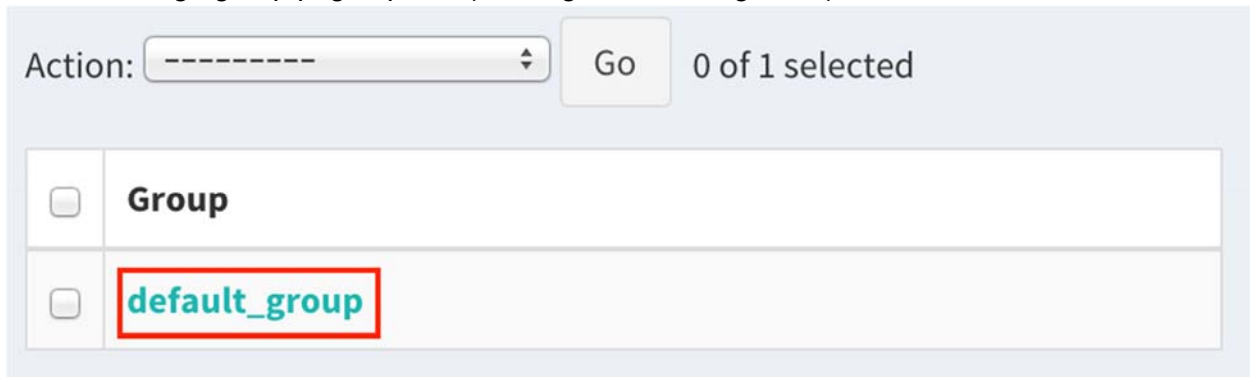


Figure 6: Click the group's name

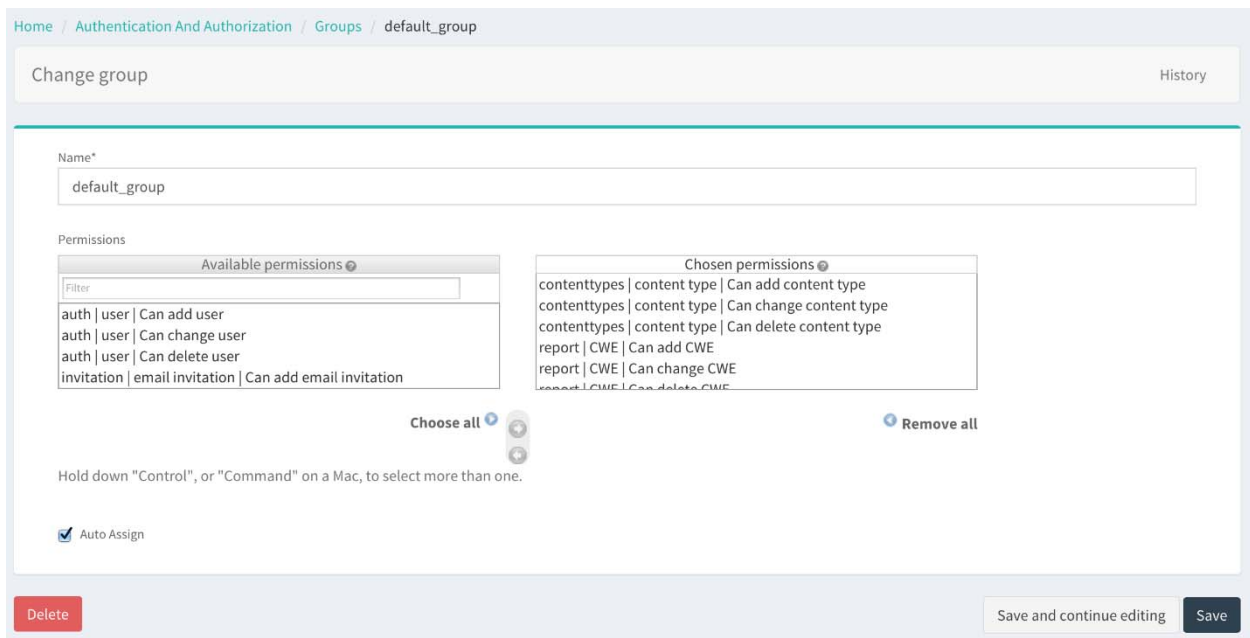


Figure 7: The Change group page opens

Delete

There are two ways to delete a user group: delete selected user groups or delete the opened user group.

To delete the selected user groups, follow the steps below:

1. In the dashboard page, navigate to the user group list through “Authentication and Authorization” -> “Groups”.
2. Select all the user groups to be deleted.
(See Figure 8 and Figure 9.)

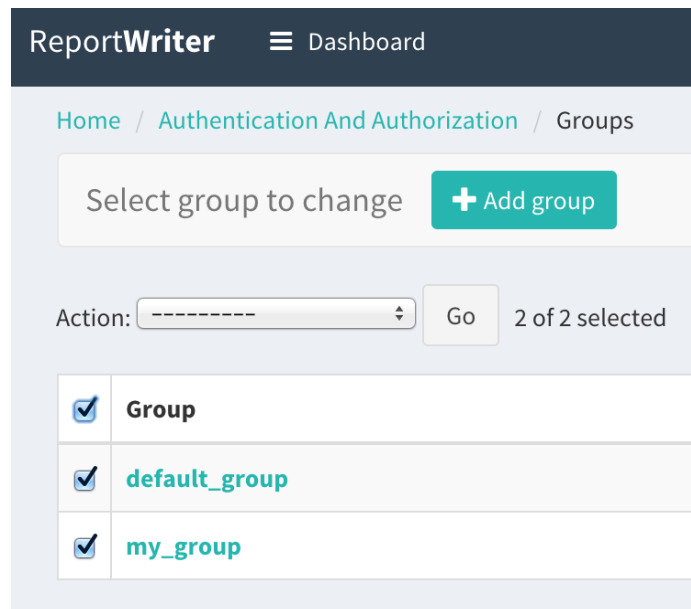


Figure 8: Select user group for deletion

3. Select “Delete selected groups” from the drop-down list.

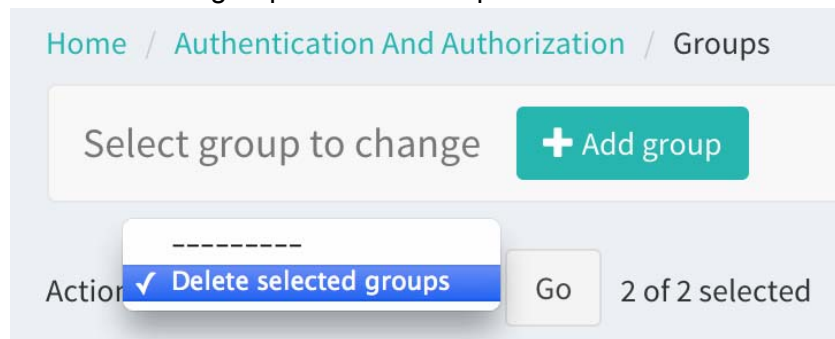


Figure 9: Delete user group

4. Click the “Go” button. A confirmation page displays.
5. Click “Yes, I’m sure” to delete all the selected groups, or click “No, take me back” to return to the group list page.

To delete the opened user group, follow the steps below:

1. In the dashboard page, navigate to the user group list through “Authentication and Authorization” -> “Groups”.
2. Click the group name to open the group.
3. In the group page, click the “Delete” button.
4. Click “Yes, I’m sure” to delete this group, or click “No, take me back” to return to the group page.

Save

You can save a group that has been edited by using any of these three buttons: “Save and add another”, “Save and continue editing”, or “Save”.

These three buttons are usually visible in the group detail page. However, “Save and add another” is only visible when you are adding a new group.

The function of each button is described below:

- **Save and add another:** The currently edited group is saved and a page with all the fields of the default values displays so you can add another group.
- **Save and continue editing:** The currently edited group is saved and remains open. You can continue editing its information.
- **Save:** The currently edited group is saved. The group list page displays.

Tasks

This section describes the steps for completing the tasks you perform most frequently.

Log in

To log in to the system, follow the steps below:

1. Open the home page of the website.
2. Click the “Log in” button on the top-right corner.

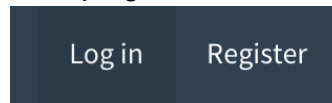


Figure 10: Log in

3. Enter your username and password.

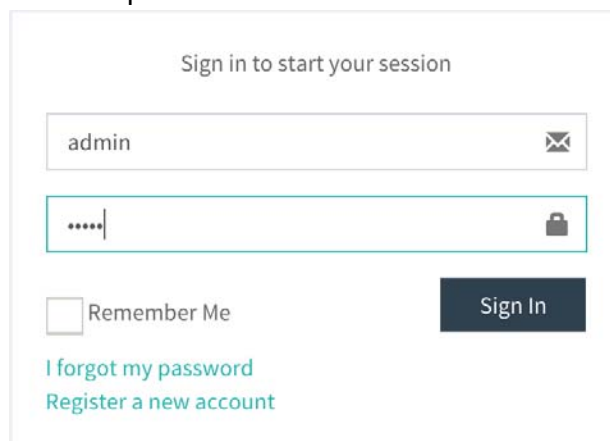


Figure 11: Sign in

4. Click the “Sign In” button.
5. When the dashboard page displays, you have logged in successfully.

Log out

To log out of the system, follow the steps below:

1. In any page, click the user icon in the top-right corner. A drop-down menu displays.

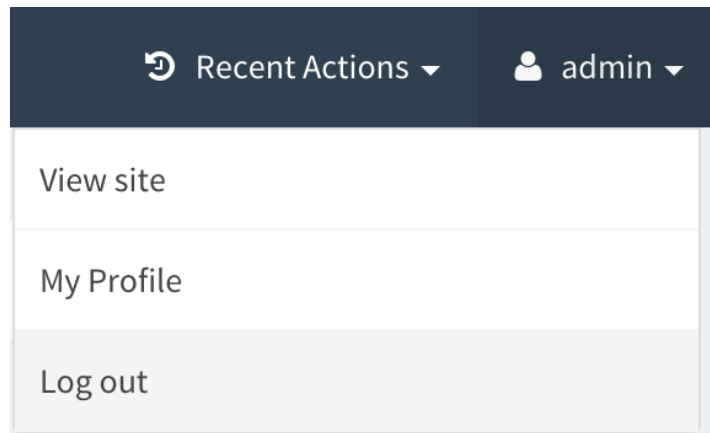


Figure 12: Log out

2. Click “Log out”.
3. A confirmation page displays to confirm that you intend to log out.

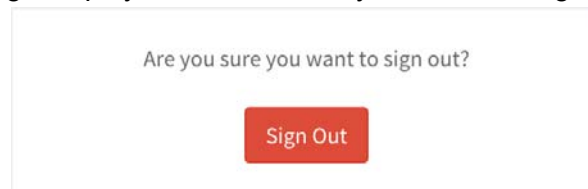


Figure 13: Confirm logout

NOTE: If you do not wish to log out, click the “Dashboard” button on the top of the page to return to the dashboard page.

4. Click “Sign Out”.
5. The home page displays. The “Log in” button displays on the top-right corner, which means you have logged out successfully.

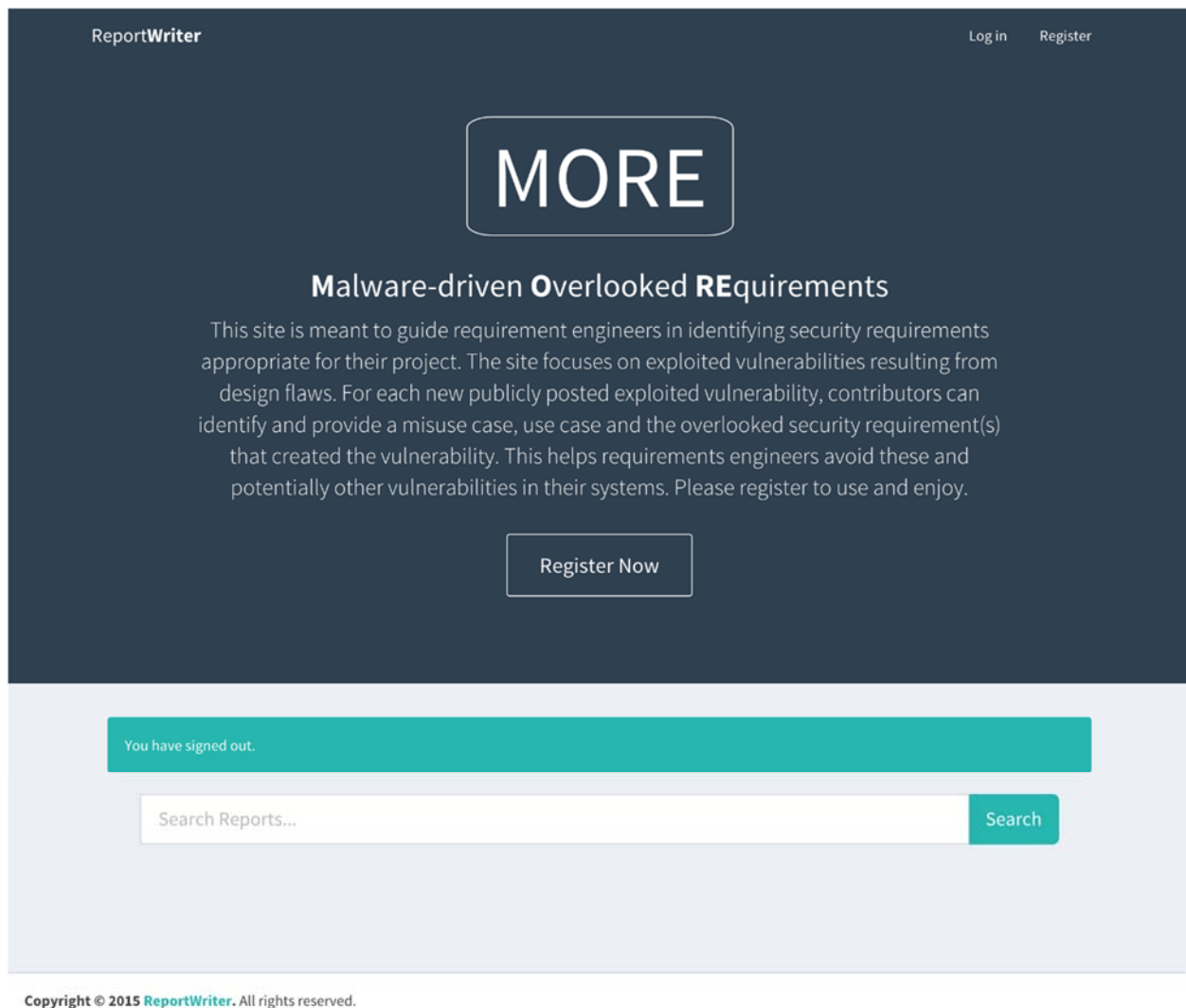


Figure 14: Home page

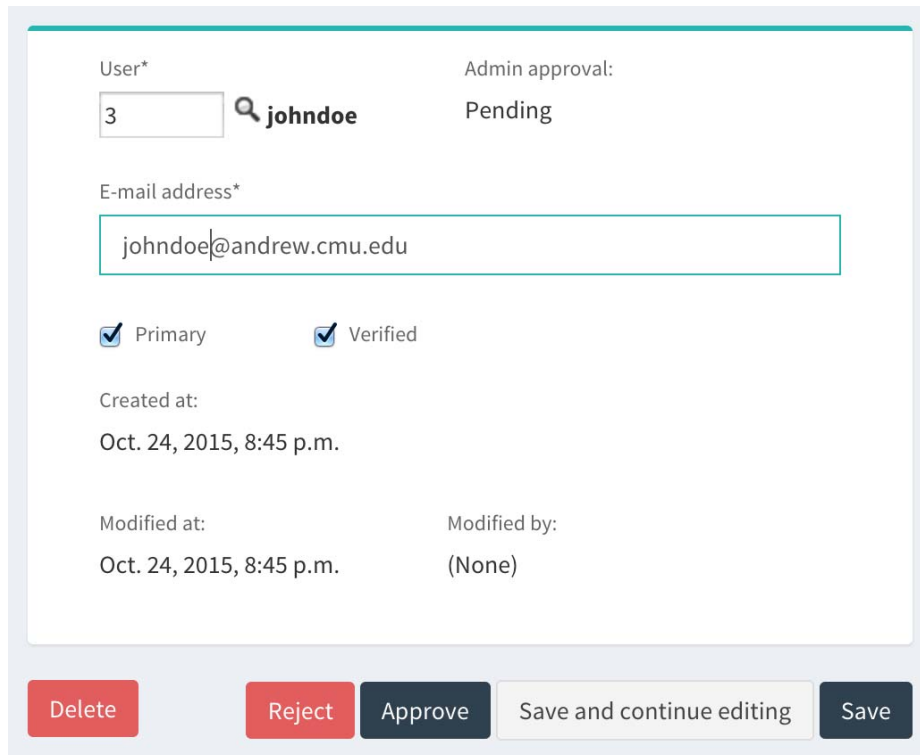
Approve New User's Registration

Scenario: The user has registered and verified his/her email, but still cannot log in.

To approve a user's registration, follow the steps below:

1. In the dashboard page, navigate to "Accounts" -> "Email addresses".
2. In the email address list, click the email address to be approved. The value of the "Admin approval" of this email should be "Pending".
3. In the "Change email address" page, click "Approve" to approve this email address.

(See Figure 15.)



User* 3 johndoe Admin approval: Pending

E-mail address* johndoe@andrew.cmu.edu

☒ Primary ☒ Verified

Created at:
Oct. 24, 2015, 8:45 p.m.

Modified at: Oct. 24, 2015, 8:45 p.m. Modified by: (None)

Delete Reject Approve Save and continue editing Save

Figure 15: Approve email address

4. After the email address is approved, a message displays.

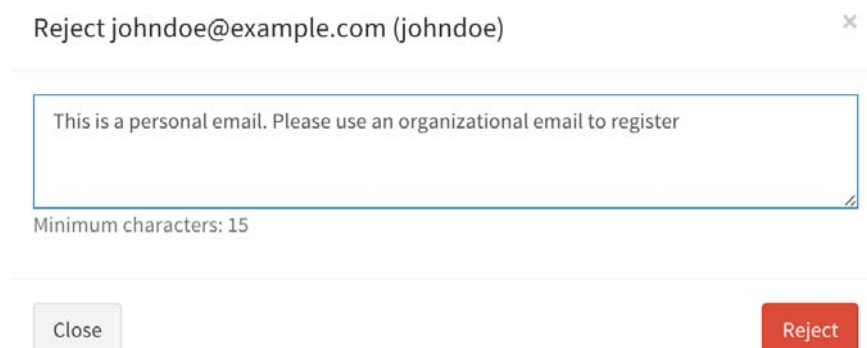
The email address "johndoe@andrew.cmu.edu (johndoe)" has been approved.

Figure 16: Email address approval confirmation

5. The user can now log in.

Alternatively, follow the steps below if you wish to reject the registration of the user:

1. In Step 3, click "Reject".
2. Enter the reason for rejecting the user's registration in the pop-up dialog.



Reject johndoe@example.com (johndoe) ✕

This is a personal email. Please use an organizational email to register

Minimum characters: 15

Close Reject

Figure 17: Reject registration

3. Click “Reject”.
4. The following message displays.

This request has been rejected : This is a personal email. Please use an organizational email to register.

Figure 18: Rejection email

5. The user receives an email that explains why the request is rejected.

Privilege Management

Group Management

To add a group, follow the steps below:

1. In the admin dashboard, navigate to “Authentication and Authorization” -> “Groups”.
2. In the group list page, click “Add group”.
3. In the “Add group” page, enter the group name.
4. In the “Permissions” list box, select the permissions that should be assigned to the group.

Permissions

Available permissions ⓘ		
Filter		
cwe	Category	Can add Category
cwe	Category	Can change Category
cwe	Category	Can delete Category
cwe	Category	Can view Category

Figure 19: Select group permissions

5. Click the right arrow to assign the selected permissions to the user.


Before permission assignment:	<div> <div>Permissions</div> <div> <div>Available permissions ⓘ</div> <div>Filter</div> <div> cwe Category Can add Category cwe Category Can change Category cwe Category Can delete Category cwe Category Can view Category </div> </div> <div>Choose all ⓘ </div> </div>
After permission assignment:	<div> <div>Chosen permissions ⓘ</div> <div> cwe Category Can add Category cwe Category Can change Category cwe Category Can view Category </div> </div>

Figure 20: Assign group permissions

6. If the a user should be automatically assigned to this group, choose one or more of the following:
 - a. **Auto Assign:** This group will be automatically assigned to any registered user.
 - b. **Auto Assign to Clients:** This group will be automatically assigned to any registered client.
 - c. **Auto Assign to Contributors:** This group will be automatically assigned to any registered contributor.
7. Click “Save” to save the permission assignment.

To modify a group’s configuration, follow the steps below:

1. In the admin dashboard, navigate to “Authentication and Authorization” -> “Groups”.
2. In the group list page, click the group name.
3. Modify the permissions or the automatic assignment options in the way described above.
4. Click “Save” to save the modifications.

User Management

To manage the user’s permissions, follow the steps below:

1. In the admin dashboard, navigate to “Authentication and Authorization” -> “Users”.

2. In the user list page, click the user's name.
3. In the "Change user" page, scroll down to the "Permissions" section.
4. In the "User permissions" list box, select the permissions to be assigned to the user.

User permissions

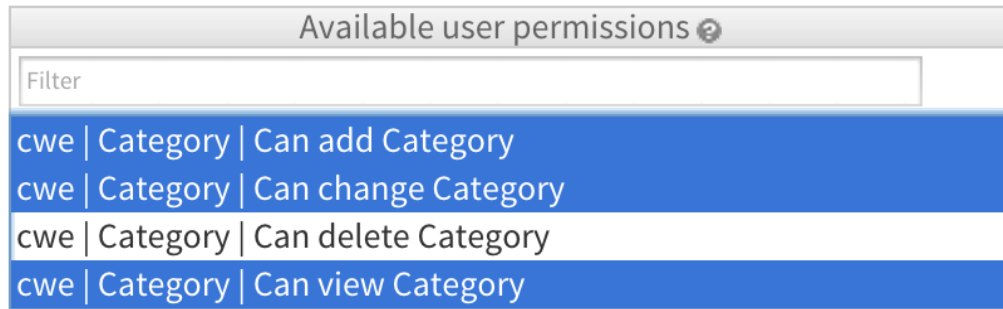


Figure 21: Select user permissions

5. Click the right arrow to assign the selected permissions to the user.

User permissions

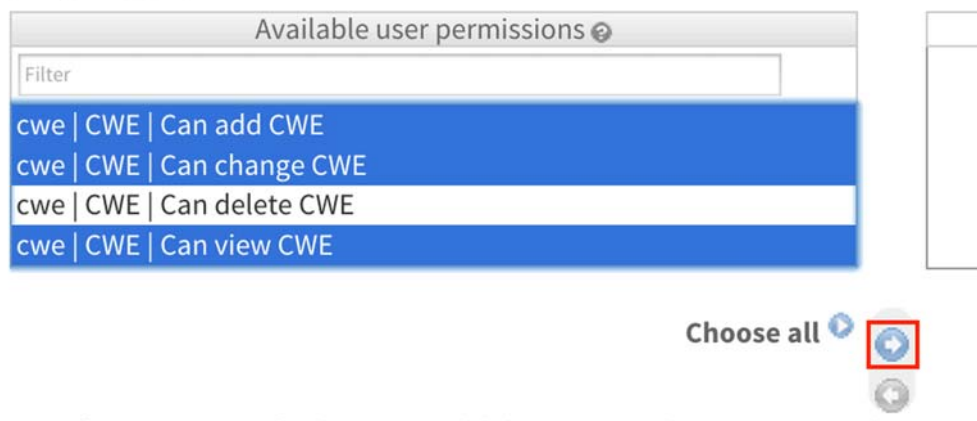


Figure 22: Before permission assignment

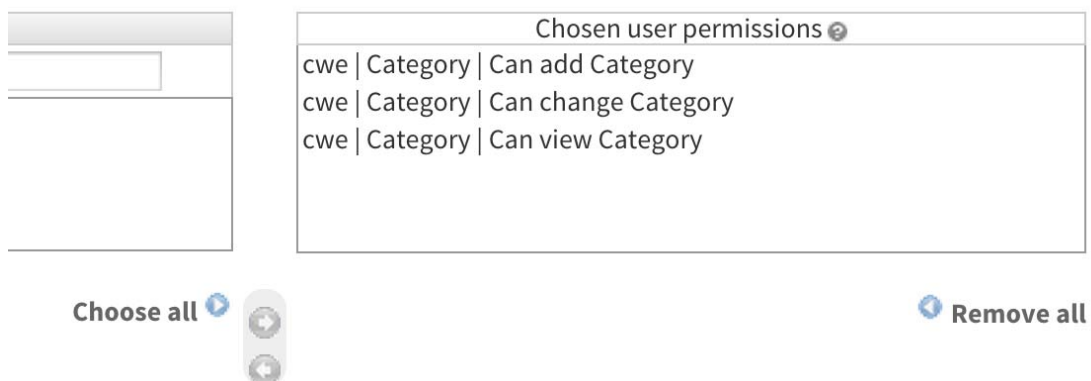


Figure 23: After permission assignment

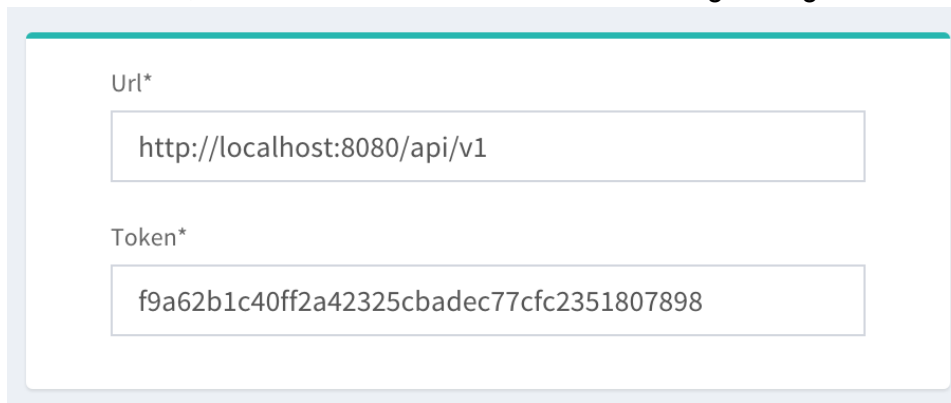
6. Click “Save” to save the permission assignment.

REST API Management

Because the Report Writer application must communicate with the SERF server via REST API, you must manage REST configuration so the Report Writer application can function correctly.

To manage the REST API configuration, follow the steps below:

1. In the admin dashboard, navigate to “REST API” -> “REST Configuration”.
2. In the “Change REST Configuration” page
 - a. In “Url”, enter the URL of the SERF server plus “/api/v1”. Please do not append “/” after “v1”.
 - b. In “Token”, enter the token that is obtained after registering as a client in SERF.



The screenshot shows a form titled "Change REST Configuration" with two input fields. The first field is labeled "Url*" and contains the text "http://localhost:8080/api/v1". The second field is labeled "Token*" and contains the text "f9a62b1c40ff2a42325cbadec77cfc2351807898".

Figure 24: Change REST configuration

3. Click “Save” to save the site information.

Security Requirements Finder User Manual

Security Requirements Finder (SERF) User Manual

Table of Contents

Introduction	51
Roles.....	51
Public User	51
Who is a public user?	51
Viewing existing MUOs	51
Searching existing MUOs	53
Contributors and Reviewers.....	53
Contributor	54
Registration	54
After login.....	56
Actions performed by a contributor.....	57
Reviewer.....	63
Client	64

Introduction

Security Requirement Finder (SERF) is an application that allows contributors to add misuse cases, use cases, and overlooked security requirements (MUO) to listed security vulnerabilities associated with reported malware attacks (Common Weakness Enumeration). By enabling the report writers to provide reports with increased comprehensive content in a certain format, SERF also enables the requirement engineers and system architects who view the reports to prevent the same security issues from recurring.

This document is the user manual for the SERF website. It describes the detailed steps users should take to accomplish their everyday tasks.

Roles

Four primary roles will use the Security Requirements Finder Application:

1. public user
2. contributor
3. reviewer
4. client

There is also one admin super user associated with the SERF Application. Please refer to the SERF Admin guide for more information about the operations an admin can perform. This SERF user manual only lists the features specifically accessible to a public user, contributor, and reviewer.

Public User

Who is a public user?

A public user is any user who wishes to view the existing use cases, misuse cases, and overlooked security requirements in the application. This user might be a requirements engineer or a software architect who is writing or listing the requirements for a software project. He or she can either search for a particular MUO related to a specific Common Weakness Enumeration (CWE) or view all the existing MUOs in the system. The instructions below are geared to the public user.

Viewing existing MUOs

To view the existing MUOs, perform the following steps:

1. Launch the URL <http://serf-sei.herokuapp.com/>
The following page displays. (See Figure 1.)

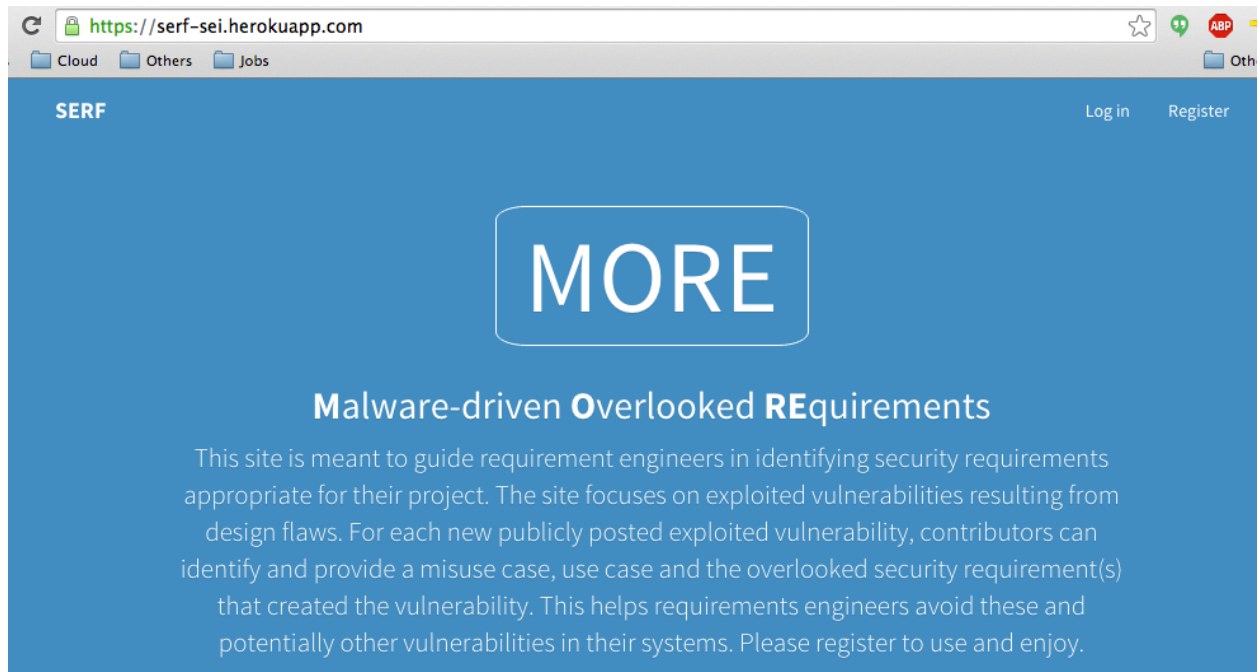


Figure 1

2. To view the existing MUOs, scroll down the page to locate the “Get MUOs” button. (See Figure 2.)

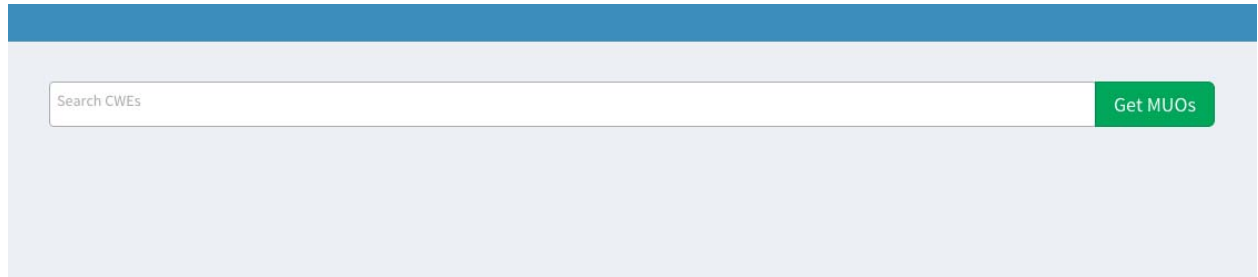


Figure 2

3. Click the “Get MUOs” button. The existing MUOs display. Ideally the screen should appear as below. (See Figure 3.) To view additional MUOs, scroll down the left and right panes.

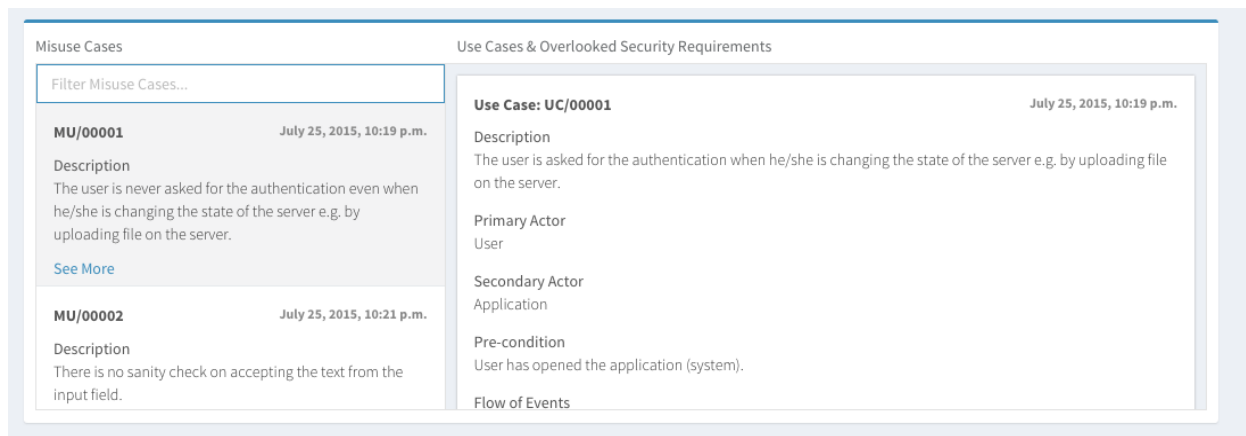


Figure 3

Searching existing MUOs

As a public user, you can also search for an MUO by typing the name of any relevant CWE you are aware of. When you type the CWE, the screen displays a list of related CWEs from which to choose. The list looks similar to the one below. (See Figure 4.)

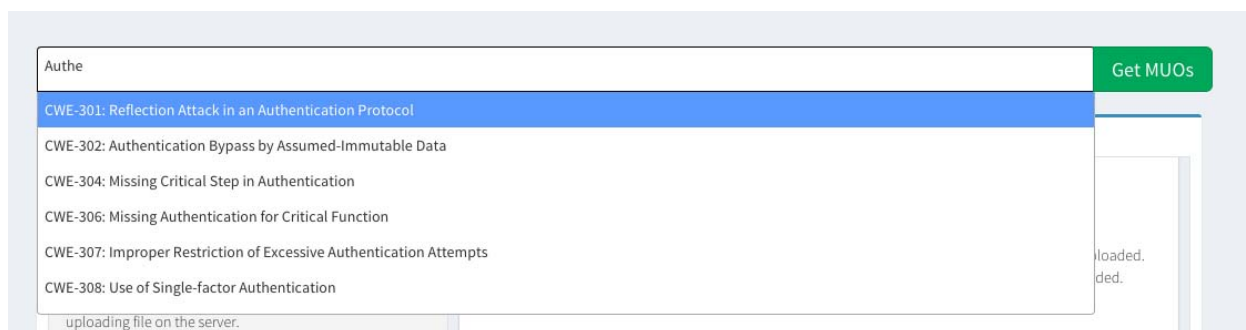


Figure 4

For example, when you type Authentication, a list of CWEs related to Authentication displays as shown. You can choose one of them and view the related MUOs for the selected CWE.

Contributors and Reviewers

Any public user who wishes to contribute to the website can do so in one of the following ways:

- Become a contributor and write MUOs.
- Become a reviewer and review the MUOs.

Contributor

Should you wish to become a contributor, you must first register as contributor and then log into the system. The registration process is explained below.

Registration

To register as a contributor, follow the steps below:

1. Click on the “Register” button in the top right corner as shown below. (See Figure 5.)

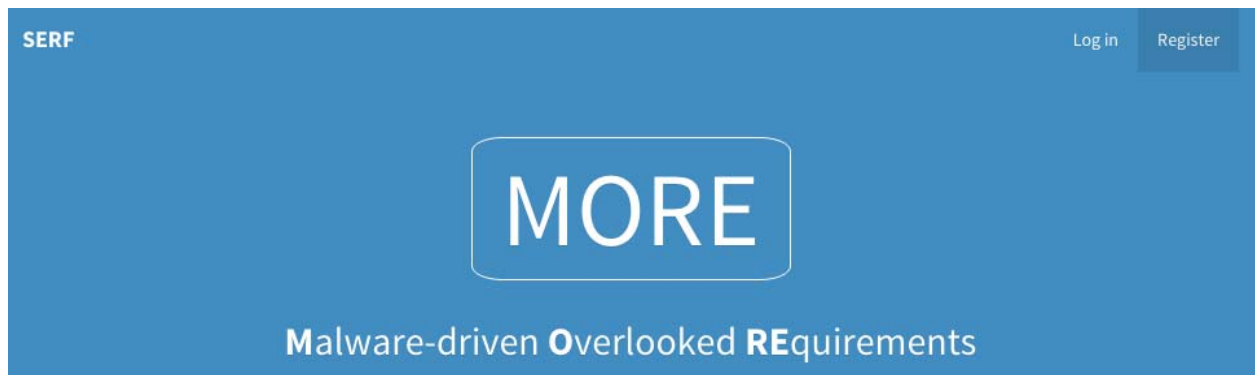


Figure 5

2. A screen like the one below will appear. (See Figure 6.) Fill in your details and make sure you choose your role as a contributor.

The image shows a 'Sign Up' form. At the top, it says 'Sign Up' in a light blue header. Below the header, there is a link: 'Already have an account? Then please [sign in](#).' The form contains several input fields: 'Username*' with a placeholder 'Username', 'First name*' with a placeholder 'First name', 'Last name*' with a placeholder 'Last name', 'Password*' with a placeholder 'Password', 'Password (again)*' with a placeholder 'Password (again)', and 'E-mail*' with a placeholder 'E-mail'. Below these fields is a 'Role*' section with two radio buttons: 'Contributor' (selected) and 'Client'. At the bottom, there is a section labeled 'I'm a human*' containing a CAPTCHA image of a green street sign with the number '9' and the letter 'S'.

Figure 6

3. After entering your details, make sure you click the “Sign-Up” button, which is located at the bottom left of the page. (See Figure 7.)

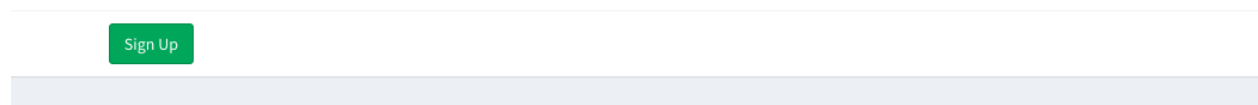


Figure 7

A typical completed form displays as below. (See Figure 8.)

A registration form with the following fields and values: Username* (Contributor), First name* (John), Last name* (Doe), Password* (*****), Password (again)* (*****), E-mail* (john.doe@gmail.com), Role* (Contributor selected), and I'm a human* (reCAPTCHA challenge). A green "Sign Up" button is at the bottom left.

Figure 8

4. After you sign up, the page below displays. (See Figure 9.) You receive a confirmation link through the email address with which you registered.

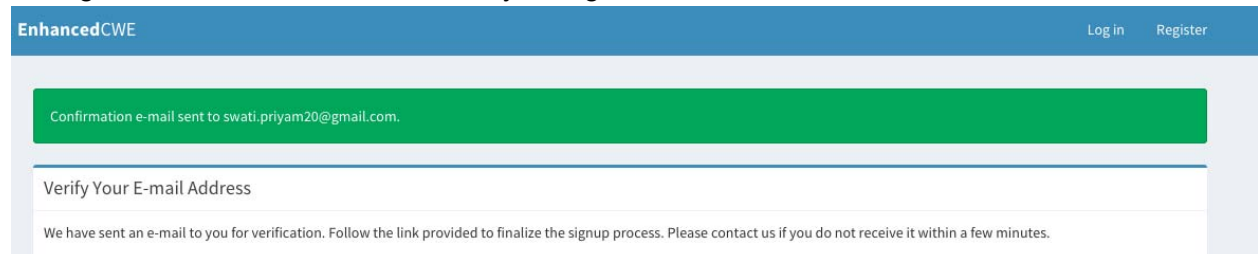


Figure 9

5. Follow the steps mentioned in the email that you receive and confirm your email address. After you confirm, a web page displays. (See Figure 10.)

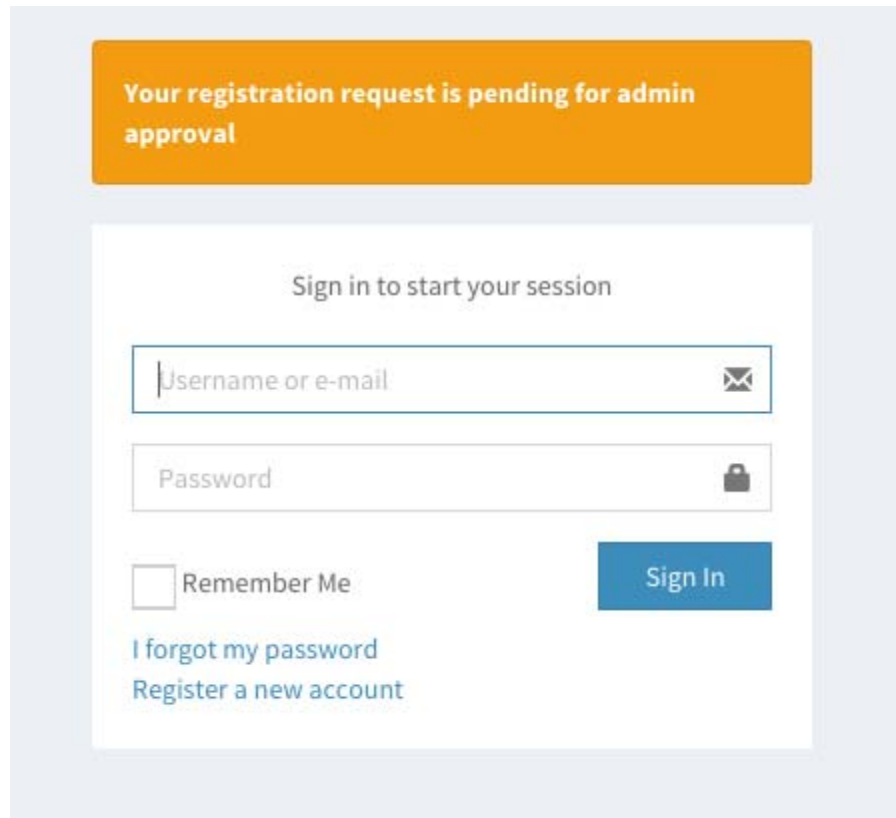


Figure 10

6. Wait for the admin to approve your registration. You will receive an email notifying you when admin approval is complete.
7. After the admin approves, you are set to perform all operations as a contributor!

After login

After you register successfully, the dashboard displays. (See Figure 11.) You can see CWE and MUO listed on the dashboard.

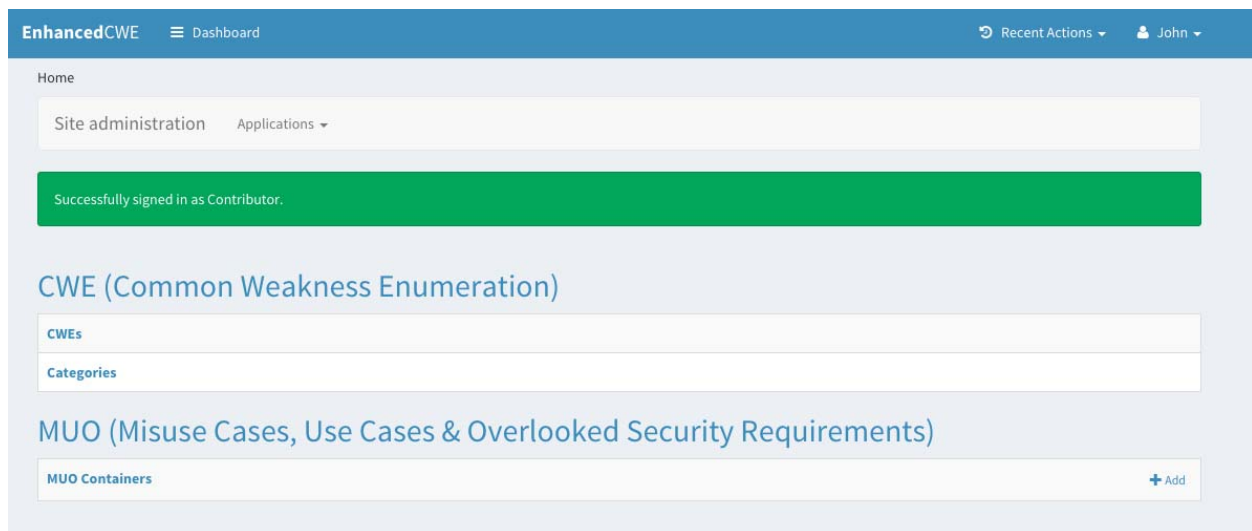


Figure 11

Actions performed by a contributor

CWEs and Category

1. A contributor can view existing CWEs and category information stored in the system. (See Figure 12.)

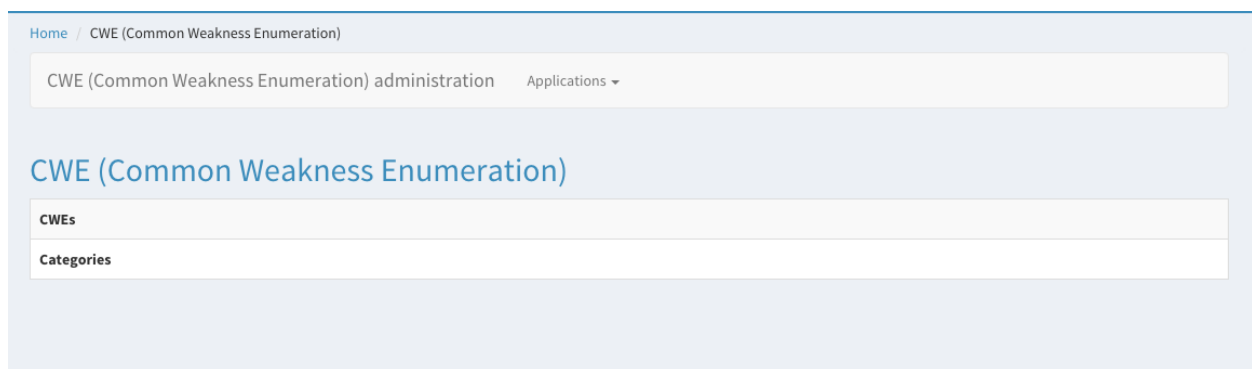


Figure 12

2. A list of CWEs displays. (See Figure 13.)

CWE
CWE-99: Improper Control of Resource Identifiers ('Resource Injection')
CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')
CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page
CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')
CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')
CWE-942: Overly Permissive Cross-domain Whitelist
CWE-941: Incorrectly Specified Destination in a Communication Channel
CWE-940: Improper Verification of Source of a Communication Channel
CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection')
CWE-927: Use of Implicit Intent for Sensitive Communication
CWE-926: Improper Export of Android Application Components
CWE-925: Improper Verification of Intent by Broadcast Receiver
CWE-921: Storage of Sensitive Data in a Mechanism without Access Control
CWE-920: Improper Neutralization of Base Conversion

Figure 13

3. As contributor, you can select a particular CWE to view or change. An example of a particular CWE appears below. (See Figure 14.)

CWE
<div>Code:</div> <div>99</div> <div>Name:</div> <div>Improper Control of Resource Identifiers ('Resource Injection')</div> <div>Description:</div> <div>The software receives input from an upstream component, but it does not restrict or incorrectly restricts the input before it is used as an identifier for a resource that may be outside the intended sphere of control.</div>
Categories
Categories:

Figure 14 (partial view)

keywords

Keywords:
improp, inject, control, resourc, incorrectli, restrict, sphere, outsid, compon, softwar, intend, upstream, identifi, may, receiv, input, use

Get Keywords Suggestions

Enter text here to suggest related keywords...

Request Suggestions

Figure 14 (partial view)

4. Each CWE is related to one or more keywords. As a contributor, you can suggest a new keyword by adding the keyword suggestion and clicking the “Request Suggestions” button. The keyword-stemming algorithm will change the keyword to a smaller form as shown below. For example, if you suggest adding “Authentication” the algorithm will stem it as “Authent”, after which you can add that keyword in the system. (See Figure 15.)

Get Keywords Suggestions

Authentication

Request Suggestions

authent

Add Keywords

Figure 15

MUO Containers

1. You can add a new MUO container by clicking “Add MUO Container”. There are two ways to do this.

The first is to click the “+Add” button. (See Figure 16.) This button is available on the dashboard.

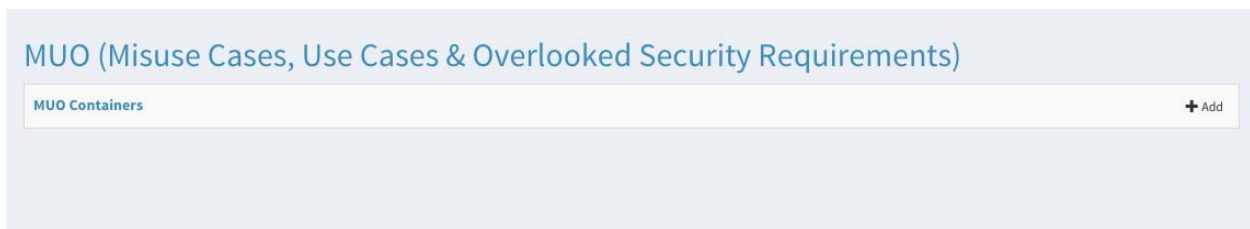


Figure 16

The second way is to click “Add MUO Container”, which appears after you click the “MUO Containers” button that appears on the dashboard. (See Figure 17.)

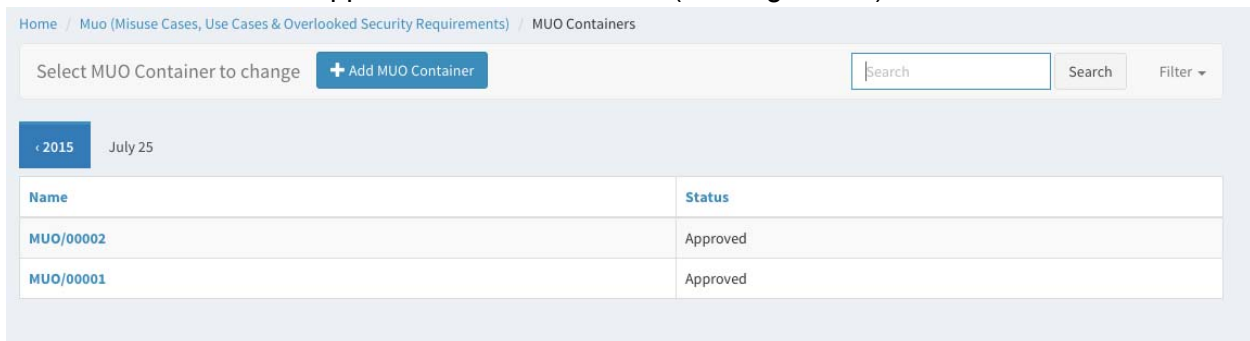


Figure 17

2. To start writing a new MUO, you must first select a related CWE. Do this by either typing the name of a specific CWE into the search box or by using the “Search” button functionality provided to the right of the search box.

The Misuse Case Type is set to New by default as a new MUO is being written. Provide a brief description of the MUO you are about to explain. (See Figure 18.)

The image shows a form for creating a new MUO. It has the following fields:

- Name:** A text input field with a "/" character.
- Cwes*:** A text input field with the placeholder "CWE..." and a search icon to the right.
- Misuse Case Type*:** A dropdown menu with "New" selected.
- Brief Description:** A large text area for writing the description.

Figure 18

Now describe the misuse case in detail by identifying the primary actor, secondary actor, pre-condition, post-condition, flow of events, assumption, and source. Typical forms resemble those below. (See Figure 19 and Figure 20.)

The form consists of three vertically stacked input fields. The first field is labeled 'Primary actor' and is a single-line text box. The second field is labeled 'Secondary actor' and is also a single-line text box. The third field is labeled 'Pre-condition' and is a larger, multi-line text box. All fields are currently empty.

Figure 19

3. Add a use case relevant to the misuse case you just described. The fields required for adding a use case are similar to the misuse case fields. Enter the brief description, primary actor, secondary actor, pre-condition, flow of events, post-condition, assumption, and source. (See Figure 20.)

#1 (Use Case)

Name:

/

Brief description

Primary actor

Secondary actor

Pre-condition

Flow of events

Post-condition

Figure 20

4. After writing the misuse case and use case(s), write the overlooked security requirement. First, choose a type of overlooked security requirement, which can be one of the following: Ubiquitous, Event-Driven, Unwanted Behavior and State-Driven. Then write the overlooked security requirement that you deem appropriate. (See Figure 21.)

Please note that you can write more than one use case for a particular misuse case, but in each use case you must mention the overlooked security requirement mentioned to complete the MUO Container entry.

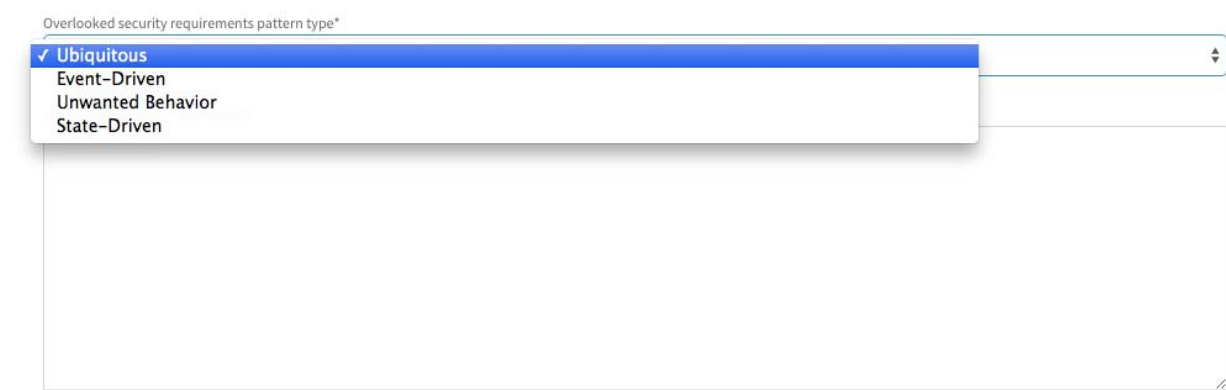
A screenshot of a web form. At the top, there is a label 'Overlooked security requirements pattern type*'. Below it is a dropdown menu. The dropdown is open, showing a list of options: 'Ubiquitous' (which is selected and has a checkmark), 'Event-Driven', 'Unwanted Behavior', and 'State-Driven'. Below the dropdown is a large, empty rectangular text area for writing the use case.

Figure 21

After you have written the MUO entry, save it by clicking the “Save” button.

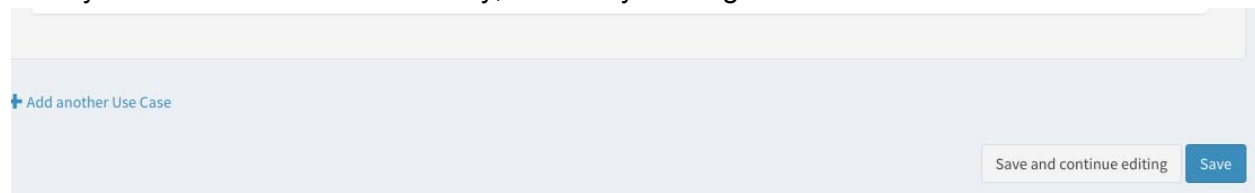
A screenshot of the bottom section of a web form. On the left, there is a link that says '+ Add another Use Case'. On the right, there are two buttons: 'Save and continue editing' and 'Save'.

Figure 22

After saving your MUO, submit it for review by clicking the “Submit for Review” button. This button is visible only after you have saved the MUO once.

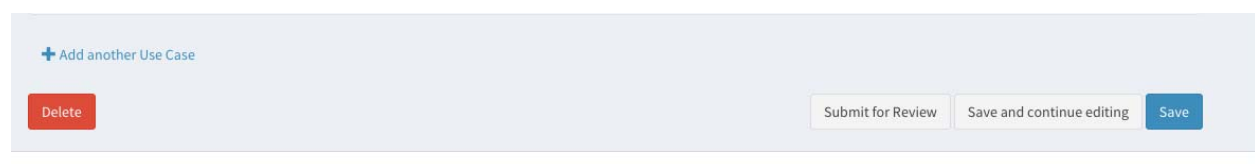
A screenshot of the bottom section of a web form, similar to Figure 22 but with an additional button. On the left, there is a link that says '+ Add another Use Case'. Below it is a red button labeled 'Delete'. On the right, there are three buttons: 'Submit for Review', 'Save and continue editing', and 'Save'.

Figure 23

After an MUO is submitted for review, all the reviewers in the system are notified. You must wait for your MUO to be accepted or rejected.

Reviewer

An admin can assign any contributor to be a reviewer. Please see the SERF Admin Guide to learn how an admin can grant reviewer rights to a contributor. If you obtain both contributor rights and reviewer rights, you can review the MUO that is submitted for review, approve/reject it, and notify the submitter by sending a relevant message.

Client

SERF provides the REST API to the Report Writer application and other similar applications (e.g., Rapid7 and ExploitDB). To access the API, Report Writer, and similar applications, the user—or any person representing the user—must register as client with the SERF to get the API token. (Once the user or user representative registers as client, an API key/token is provided to access the APIs, which is used to authenticate when these applications access the API.) To register as client, select “Client” under Role on the registration page. (See Figure 24.)

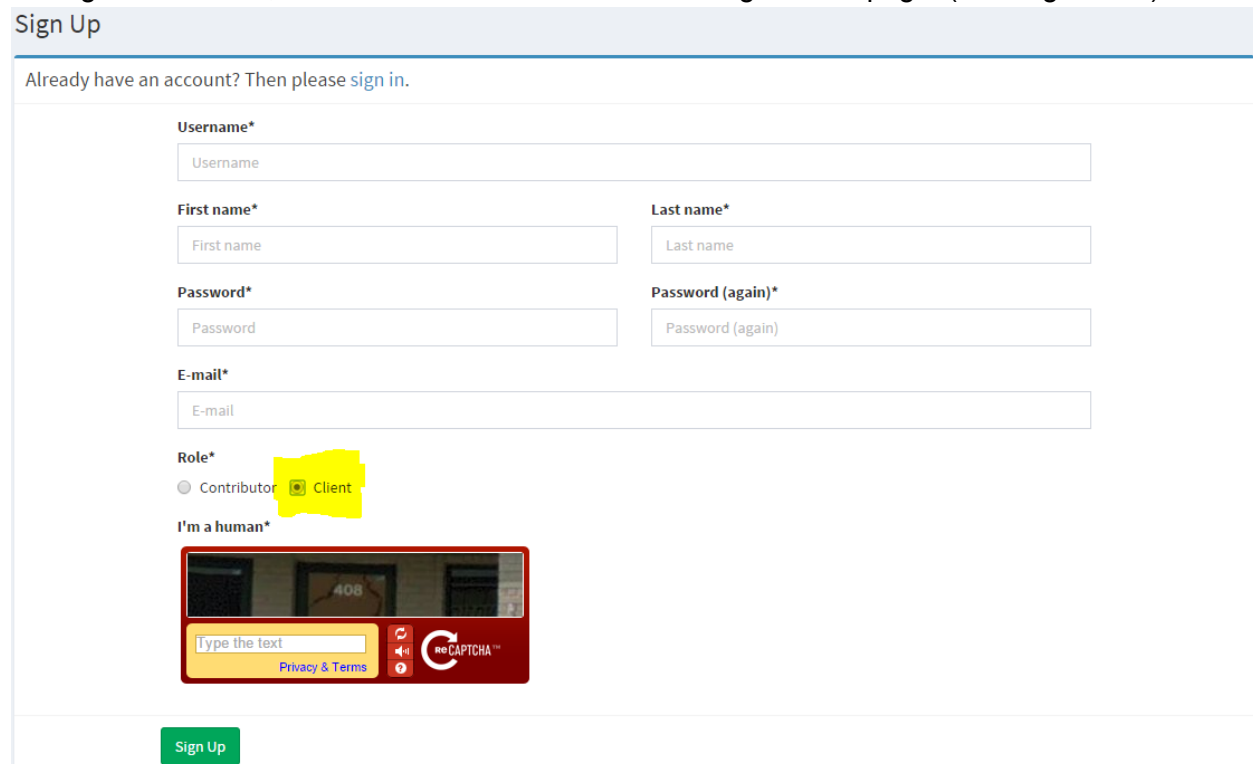
The image shows a web form titled "Sign Up" with a light blue header. Below the header, a link "Already have an account? Then please sign in." is visible. The form contains several input fields: "Username*" with a placeholder "Username", "First name*" with a placeholder "First name", "Last name*" with a placeholder "Last name", "Password*" with a placeholder "Password", "Password (again)*" with a placeholder "Password (again)", and "E-mail*" with a placeholder "E-mail". Below these is a "Role*" section with two radio buttons: "Contributor" and "Client". The "Client" radio button is selected and highlighted with a yellow rectangle. At the bottom of the form is a "Sign Up" button. A red CAPTCHA box is also present, containing a photo of a building and the text "I'm a human*", "Type the text", and "reCAPTCHA".

Figure 24

After your registration as client is confirmed, you can log in to the SERF application and copy your REST API authentication token. Do this by clicking “Tokens”. (See Figure 25.)

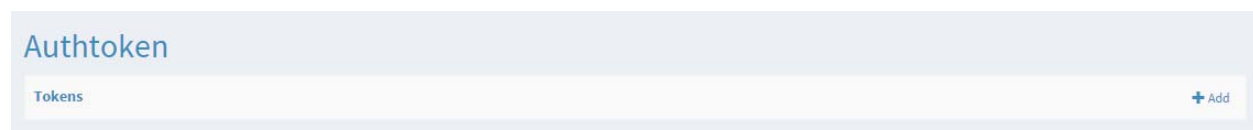
The image shows a web page titled "Authtoken" with a light blue header. Below the header, there is a section titled "Tokens" with a "+ Add" button in the top right corner.

Figure 25

When you click “Tokens”, your key displays. (See Figure 26.)



Figure 26

As client, you can copy this key and use it in your Report Writer Application's REST API settings, for a seamless communication with SERF over REST API.

Should this key become compromised, you can change it from this same screen. In this case, you must update the key at your end also (i.e., in the Report Writer application).

Security Requirements Finder Admin Guide

Security Requirements Finder (SERF) Admin Guide

Table of Contents

Introduction	71
Intended Audience	71
Common Scenarios	71
Pages	71
Home page	71
Dashboard Page	72
Common Admin Operations	73
Add	74
Modify	75
Delete	76
Save	77
Tasks	78
Login	78
Logout	78
Approve New User's Registration	80
Invite New User	82
Create an Invitation	82
Re-send Invitation	83
Access Rights Management	84
Group Management	84
User Management	85
Site Management	87

Introduction

This document is the admin guide for the web-based application Security Requirement Finder (SERF). It describes the detailed steps the application admin must follow to accomplish everyday tasks.

The document is divided into two major sections:

1. **Common Scenarios:** This section describes the frequently mentioned pages and common operations that can be shared by all the tasks.
2. **Tasks:** This section describes the detailed steps for accomplishing the everyday tasks that the website admin may need to perform.

Intended Audience

This document is intended for the admin of the SERF website.

Common Scenarios

Throughout the document, certain concepts and web pages are mentioned frequently. They are listed and defined in this section.

Pages

Home Page

The home page is the first page users see when they enter the website URL. It displays the title and a brief introduction of the website. (See Figure 1.)

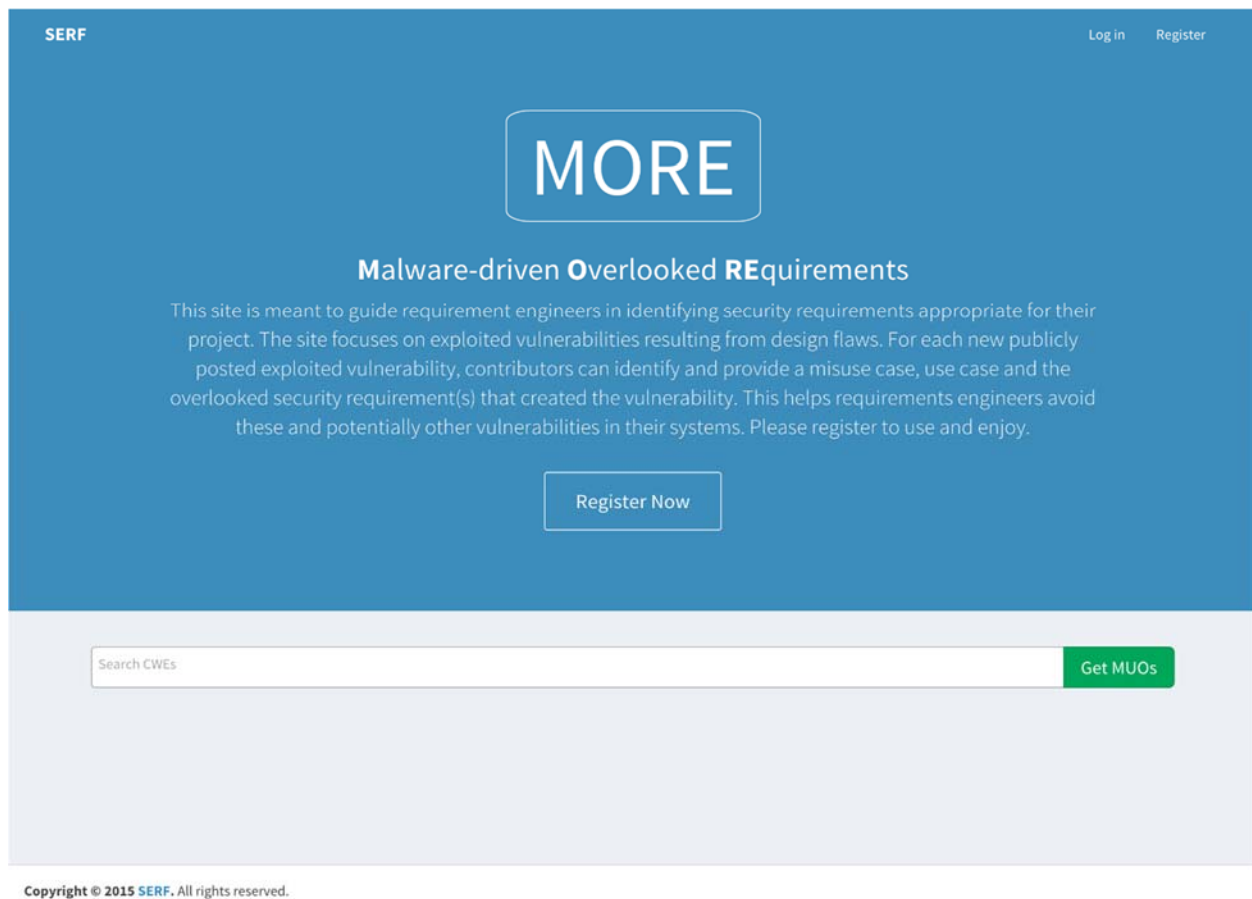


Figure 1: Home page

Dashboard Page

After logging in, you are redirected to the dashboard page, which lists all manageable task areas. (See Figure 2.)

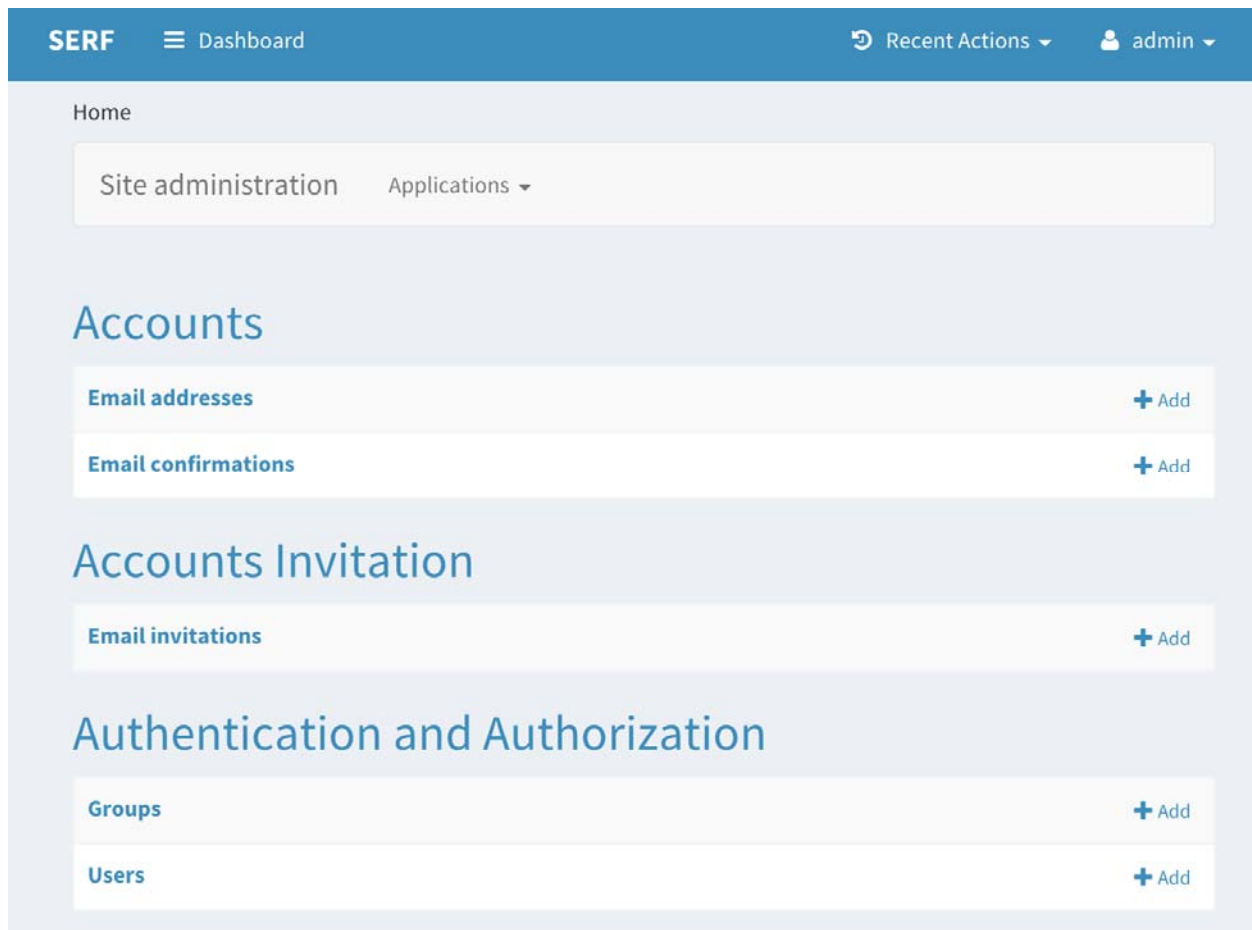


Figure 2: Dashboard Page (partial view)

Common Admin Operations

The SERF website is created with a consistent look and feel, so the management of different functions looks very similar. Each function is explained below.

The typical management operations include the following:

- **Add:** Add a new instance, such as a user group.
- **Save:** Save the current modification.
- **Modify:** Modify the information of an existing instance.
- **Delete:** Delete an existing instance.

As an example, the management of user groups will serve to show how to perform addition, modification, or deletion in the website. Beyond user groups, the four operations listed above can be applied to other managed entities, including the following:

- email addresses, email confirmations, and email invitations
- groups and users
- tokens

- CWEs, categories, and keywords
- issue Reports and MUO Containers
- sites
- user profiles

Add

You can add a user group in one of two ways: through “Add” in the dashboard page or by clicking the “Add” button in the group list page.

In the dashboard page, locate “Groups” in the “Authentication and Authorization” section. There is a “+Add” button on the right side. Click it to open the group-adding page. (See Figure 3.)

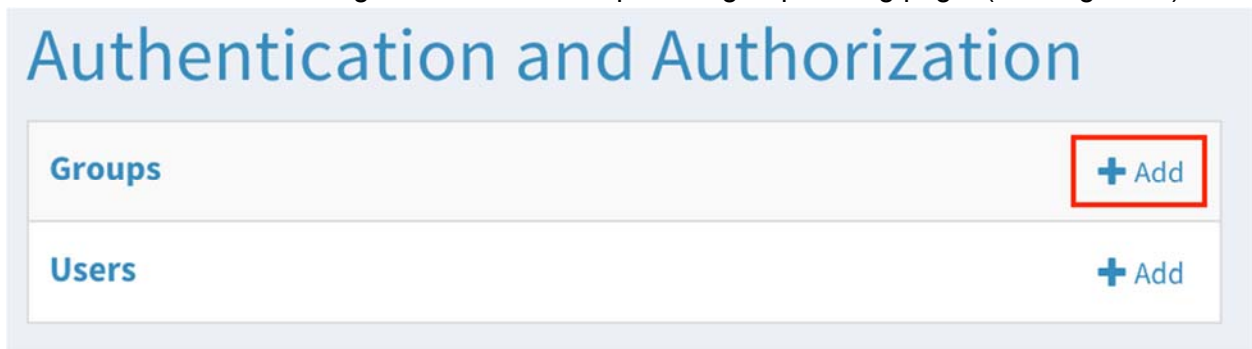


Figure 3: Add a group

Alternatively, you can click the “Groups” name first to open the group list page, then click the “Add group” button to open the group-adding page. (See Figure 4 and Figure 5.)

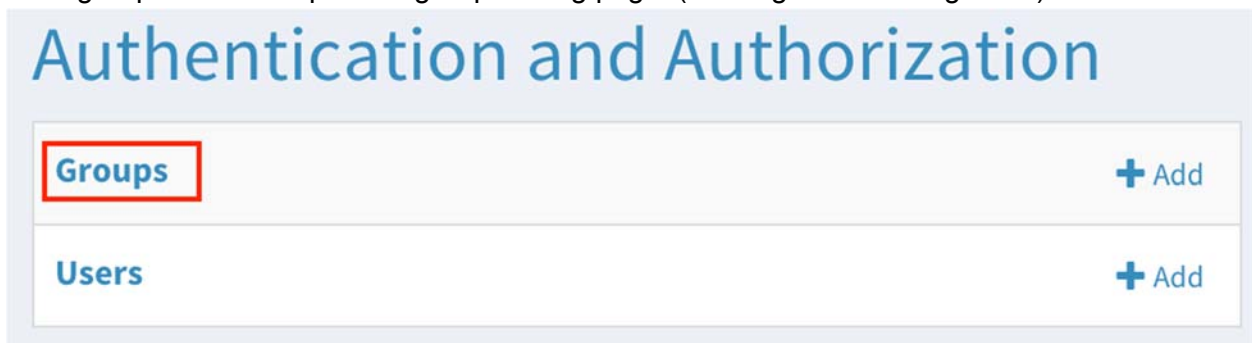


Figure 4: Click the “Groups”

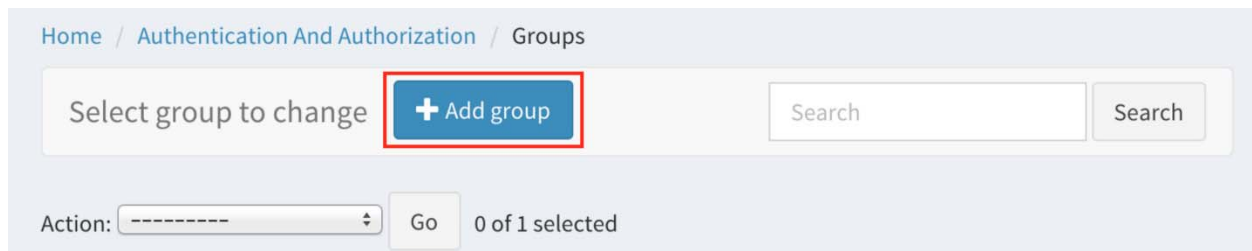


Figure 5: Click “Add group” to open the group adding page

Modify

To modify a group's settings, follow the steps below:

1. In the dashboard page, navigate to the group list page through “Authentication and Authorization” -> “Groups”. (See Figure 4 above.)
2. In the group list, click the name of the group for which information is to be changed. The “Change group” page opens. (See Figure 6 and Figure 7.)

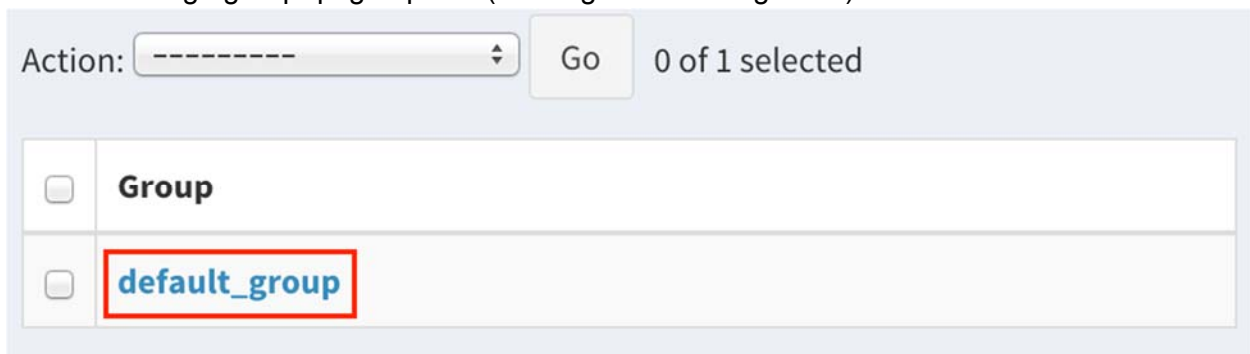


Figure 6: Click the group's name

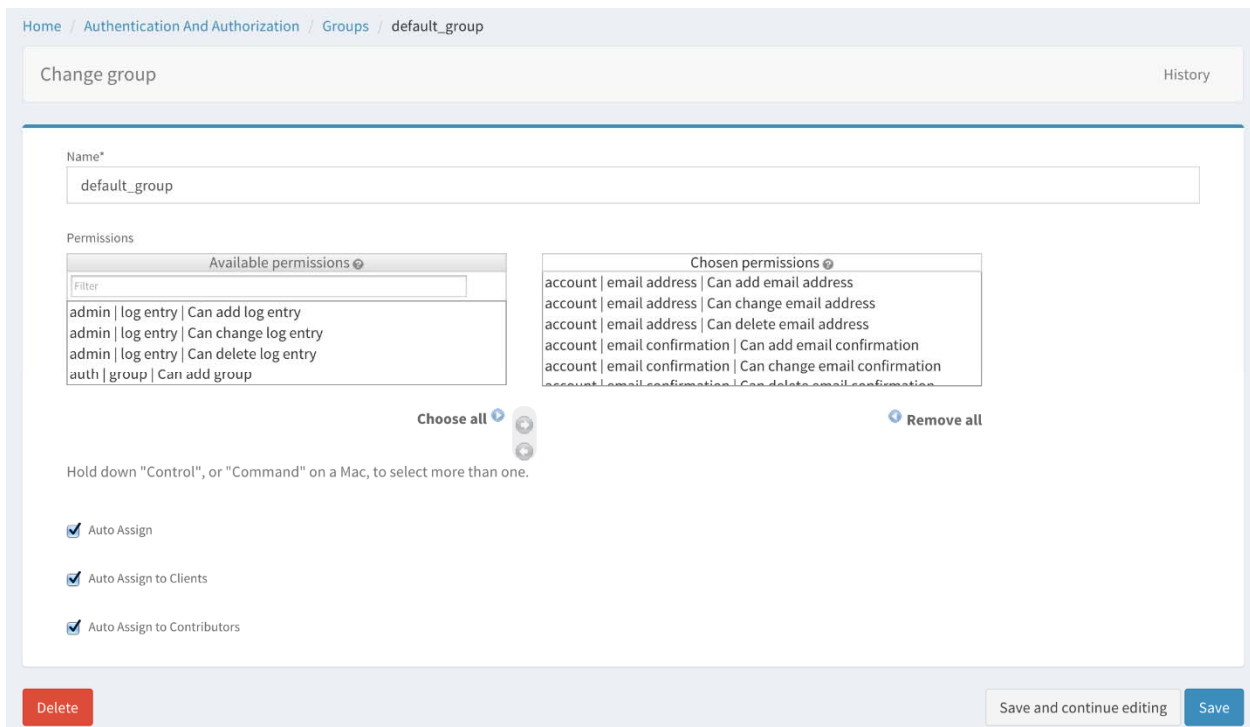


Figure 7: The “Change group” page opens

Delete

When a client unsubscribes, you must delete the user group. There are two ways to delete a user group: Delete selected user groups or delete the opened user group.

To delete the selected user groups, follow the steps below:

1. In the dashboard page, navigate to the user group list through “Authentication and Authorization” -> “Groups”. (See Figure 8.)
2. Select all the user groups to be deleted.

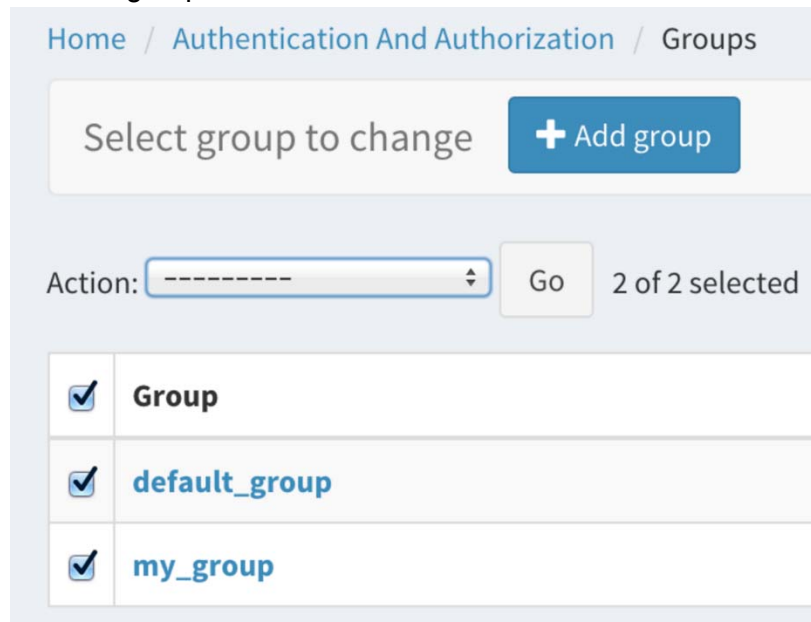


Figure 8: Select groups to be deleted

3. Select “Delete selected groups” from the drop-down list. (See Figure 9.)

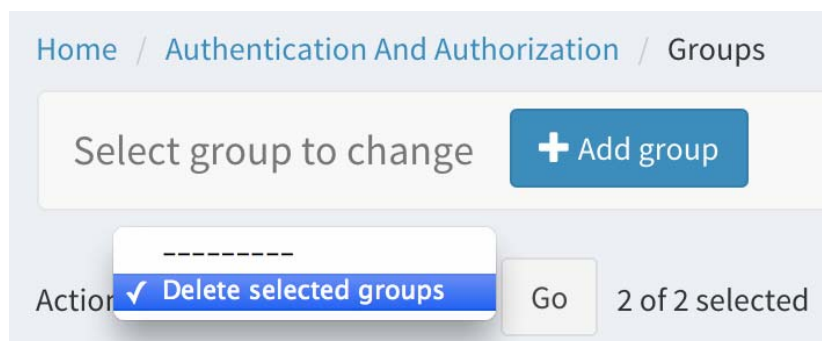


Figure 9: Delete selected groups

4. Click the “Go” button. A confirmation page displays.
5. Click “Yes, I’m sure” to delete all the selected groups, or click “No, take me back” to return to the group list page.

To delete the opened user group, follow the steps below:

1. In the dashboard page, navigate to the user group list through “Authentication and Authorization” -> “Groups”.
2. Click the group name to open the group.
3. In the group page, click the “Delete” button.
4. Click “Yes, I’m sure” to delete this group, or click “No, take me back” to return to the group page.

Save

You can save a group that has been edited by using any of these three buttons: “Save and add another”, “Save and continue editing”, or “Save”. (See Figure 10.)

Home / Authentication And Authorization / Groups / Add group

Add group

Name*

Permissions

Available permissions

Filter

- account | email address | Can add email address
- account | email address | Can change email address
- account | email address | Can delete email address
- account | email confirmation | Can add email confirmation

Choose all

Chosen permissions

Remove all

Hold down "Control", or "Command" on a Mac, to select more than one.

☐ Auto Assign

☐ Auto Assign to Clients

☐ Auto Assign to Contributors

Save and add another Save and continue editing Save

Figure 10: Save an edited group

These three buttons are usually visible in the group detail page. However, “Save and add another” is only visible when you are adding a new group.

The function of each button is described below:

- **Save and add another:** The currently edited group is saved and a page with all the fields of the default values is displayed so you can add another group.
- **Save and continue editing:** The currently edited group is saved and remains open. You can continue editing its information.
- **Save:** The currently edited group is saved. The group list page displays.

Tasks

This section describes the everyday tasks that you may need to accomplish as admin.

Login

To log in to the system, follow the steps below:

1. Open the home page of the website.
2. Click the “Log in” button on the top-right corner.



3. Enter your username and password.

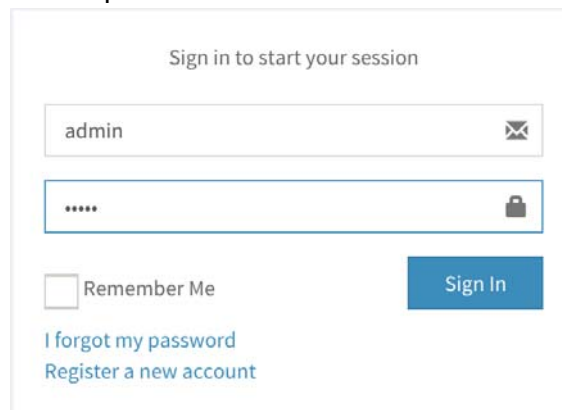
A login form titled "Sign in to start your session". It contains a username input field with the text "admin" and an email icon, a password input field with masked characters "....." and a lock icon, a "Remember Me" checkbox, a "Sign In" button, and two links: "I forgot my password" and "Register a new account".

Figure 11: Log in

4. Click the “Sign In” button.
5. When the dashboard page displays, you have logged in successfully.

Log out

To log out of the system, follow the steps below:

1. In any page, click the user icon on the top-right corner. A drop-down menu displays. (See Figure 12.)

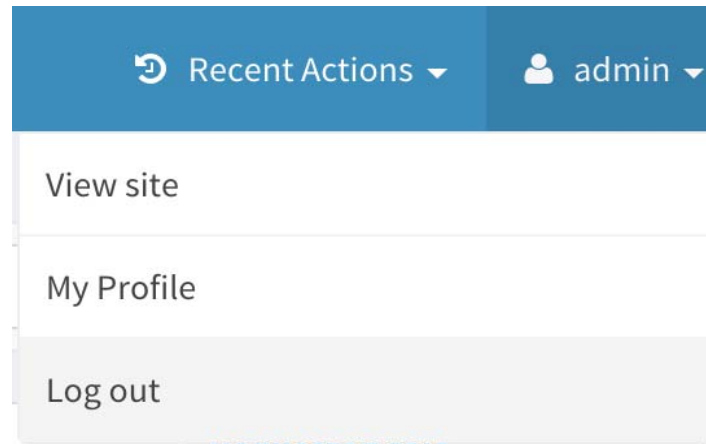


Figure 12: Click “Log out”

2. A confirmation page displays to confirm that you intend to log out.

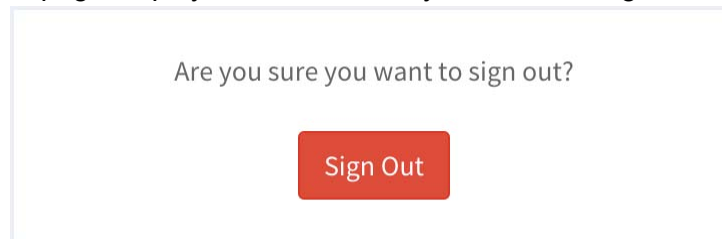
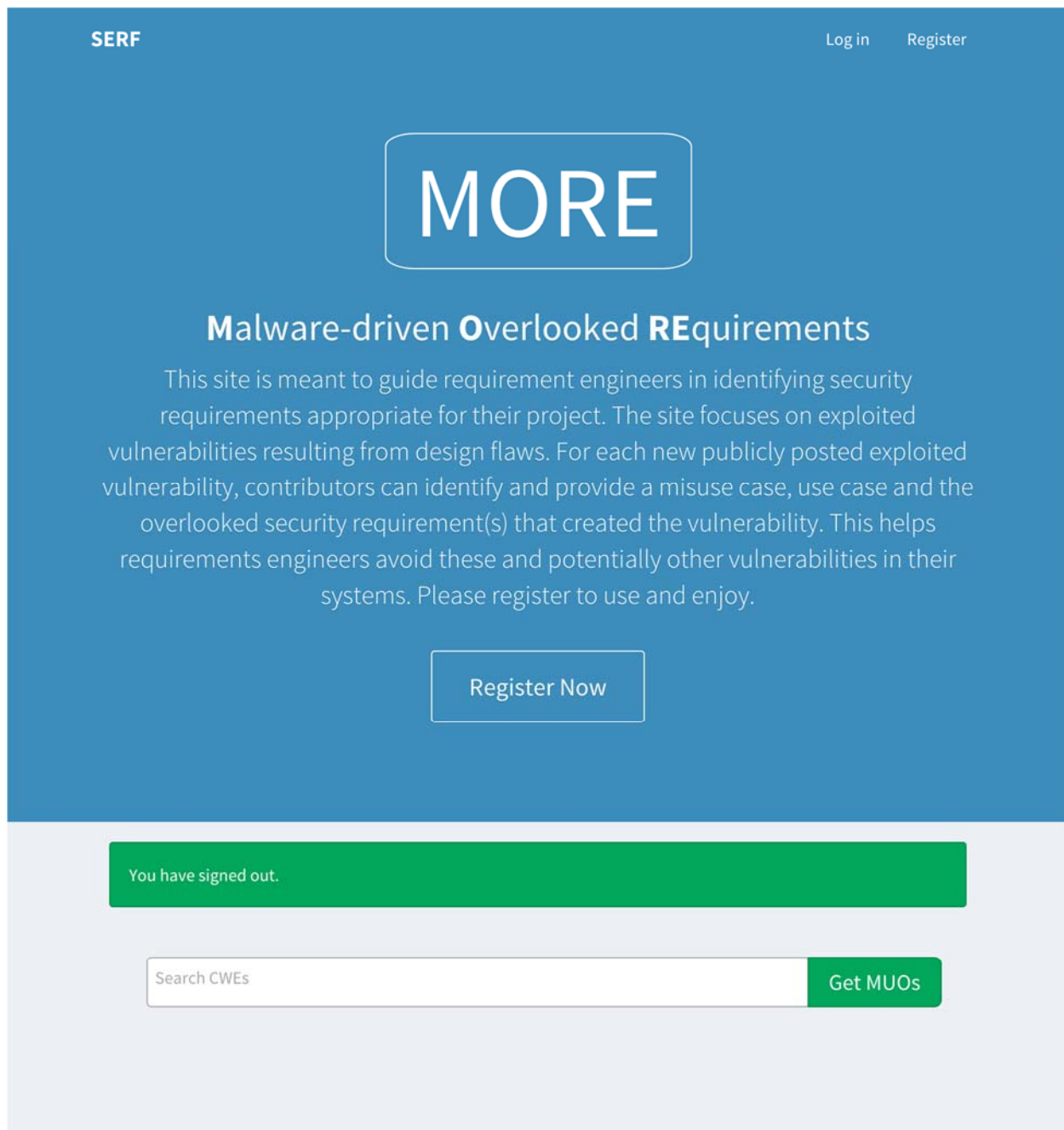


Figure 13: Click “Sign Out”

NOTE: If you do not wish to log out, click the “Dashboard” button on the top of the page to return to the dashboard page.

3. Click “Sign Out”.
4. The home page displays. The “Log in” button appears on the top-right corner, which means you have logged out successfully.



Copyright © 2015 SERF. All rights reserved.

Figure 14: Home page

Approve New User's Registration

To approve a user's registration, follow the steps below:

1. In the dashboard page, navigate to "Accounts" -> "Email addresses".

2. In the email address list, click the email address to be approved. The value of the “Admin approval” of this email should be “Pending”.
3. In the “Change email address” page, click “Approve” to approve this email address. (See Figure 15.)

The screenshot shows a web interface for managing user registration requests. At the top, there's a search bar with '5' and a magnifying glass icon, followed by the text 'johndoe'. To the right, 'Admin approval:' is listed as 'Pending'. Below this is a section for 'E-mail address*' with a text input field containing 'johndoe@example.com'. Underneath, there are two checked checkboxes: 'Primary' and 'Verified'. The 'Created at:' timestamp is 'Oct. 3, 2015, 8:36 p.m.'. The 'Modified at:' is also 'Oct. 3, 2015, 8:36 p.m.', and 'Modified by:' is '(None)'. A 'Requested role*' dropdown menu is set to 'Contributor'. At the bottom, there are five buttons: 'Delete' (red), 'Reject' (red), 'Approve' (blue), 'Save and continue editing' (light blue), and 'Save' (blue).

Figure 15: Approve registration request

4. After the email address is approved, the following message displays.

The email address "johndoe@example.com (johndoe)" has been approved.

Figure 16: Email approval message

5. The user can now log in. The user will receive an email notification about the approval.

Alternatively, follow the steps below if you wish to reject the registration of the user:

1. In Step 3, click “Reject”.
2. Enter the reason for rejecting the user’s registration in the pop-up dialog. (See Figure 17.)

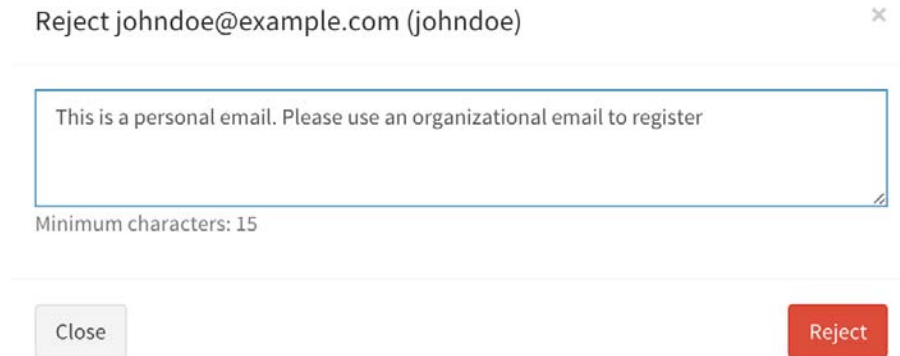


Figure 17: Reject registration request

3. Click "Reject".
4. The following message displays:

This request has been rejected : This is a personal email. Please use an organizational email to register.

Figure 18: Reason for registration rejection

5. The user receives an email that explains why the request is rejected.

Invite New User

Create an Invitation

To invite a new user to use the system, follow the steps below:

1. In the admin dashboard, navigate to "Accounts Invitation" -> "Email invitations".
2. Click "Add email invitation".
3. In the "Email" textbox, enter the email address of the user to be invited. (See Figure 19.)

Add email invitation

Email*

johndoe@example.com

Key: Status:

Pending

Created by: Created at:

(None) Oct. 3, 2015, 8:58 p.m.

Send Invitation

Figure 19: Add email invitation

4. Click “Send Invitation”.
5. The email invitation list page displays with a message of success. (See Figure 20.)

The email invitation "to johndoe@example.com" was added successfully.

< 2015 October 3

<input type="checkbox"/>	Email	Created by	Created at	Status
<input type="checkbox"/>	johndoe@example.com	admin	Oct. 3, 2015, 9:05 p.m.	Pending

Figure 20: Send email invitation

Re-Send Invitation

If the user reports that no invitation email was received or the invitation email was deleted by mistake, you can re-send the invitation email. To re-send, follow the steps below:

1. In the admin dashboard, navigate to “Accounts Invitation” -> “Email invitations”.
2. In the email list, click the email through which the owner is invited.
3. In the “Change email invitation” page, click “Re-Send Invitation”.
4. The email invitation list page will display with a message of successful re-send. (See Figure 21.)

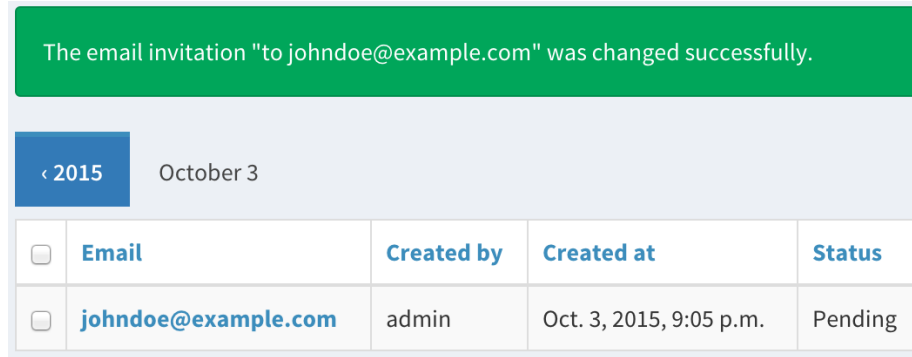


Figure 21: Successful invitation re-send

Access Rights Management

Group Management

To add a group, follow the steps below:

1. In the admin dashboard, navigate to “Authentication and Authorization” -> “Groups”.
2. In the group list page, click “Add group”.
3. In the “Add group” page, enter the group name.
4. In the “Permissions” list box, select the permissions that should be assigned to the group. (See Figure 22.)

Permissions

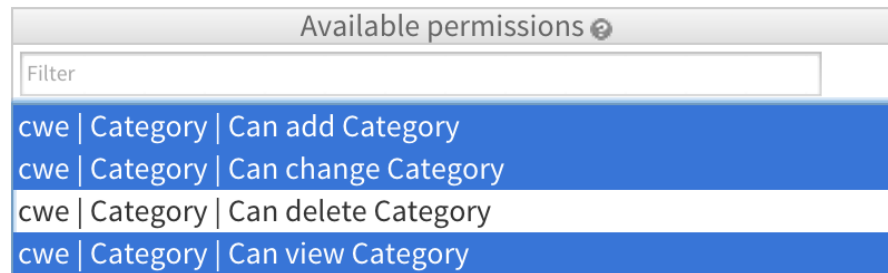


Figure 22: Select permissions

5. Click the right arrow to assign the selected permissions to the user. (See Figure 23.)



Before permission assignment:	<div> <div>Permissions</div> <div> <div>Available permissions ⓘ</div> <div>Filter</div> <div> cwe Category Can add Category cwe Category Can change Category cwe Category Can delete Category cwe Category Can view Category </div> <div>Choose all ⓘ</div> <div>   </div> </div> </div>
After permission assignment:	<div> <div>Chosen permissions ⓘ</div> <div> cwe Category Can add Category cwe Category Can change Category cwe Category Can view Category </div> </div>

Figure 23: Select permissions

6. If a user should be automatically assigned to this group, choose one or more of the following:
 - a. **Auto Assign:** This group will be automatically assigned to any registered user.
 - b. **Auto Assign to Clients:** This group will be automatically assigned to any registered clients.
 - c. **Auto Assign to Contributors:** This group will be automatically assign to any registered contributor.
7. Click “Save” to save the permission assignment.

To modify a group’s configuration, follow the steps below:

1. In the admin dashboard, navigate to “Authentication and Authorization” -> “Groups”.
2. In the group list page, click the group name.
3. Modify the permissions or the automatic assignment options as described above.
4. Click “Save” to save the modifications.

User Management

To manage the user’s permissions, follow the steps below:

1. In the admin dashboard, navigate to “Authentication and Authorization” -> “Users”.
2. In the user list page, click the user’s name.

3. In the “Change user” page, scroll down to the “Permissions” section.
4. In the “User permissions” list box, select the permissions that should be assigned to the user. (See Figure 24.)

User permissions

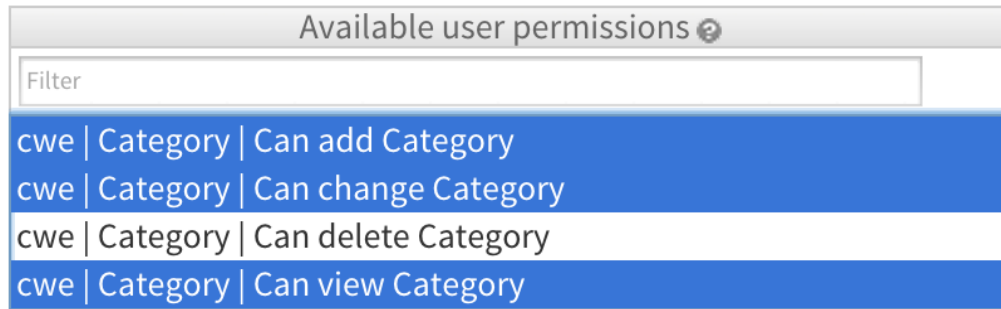


Figure 24: Change user permissions

5. Click the right arrow to assign the selected permissions to the user. (See Figure 25.)

User permissions

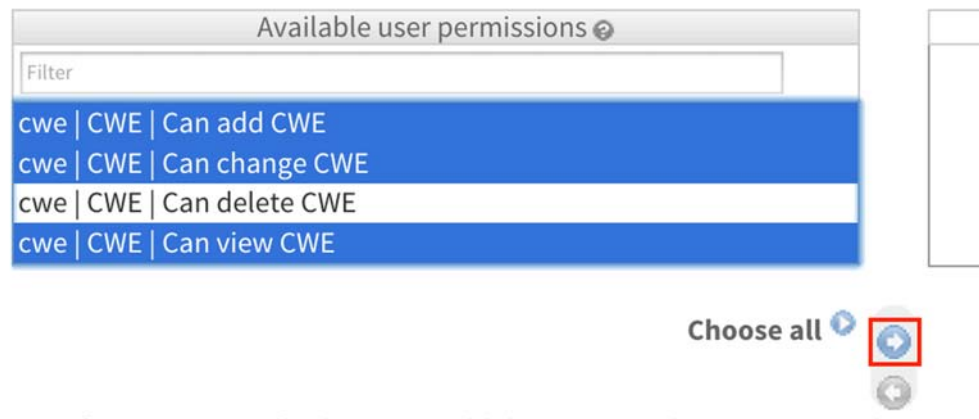


Figure 25: Before permission assignment

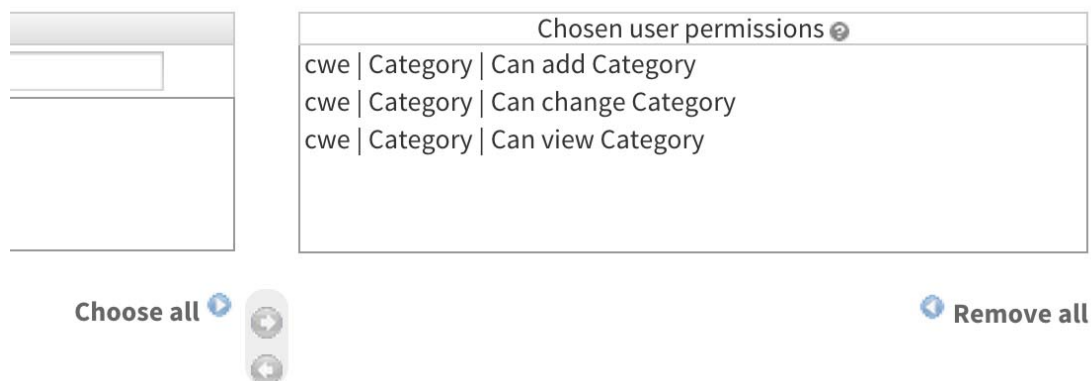


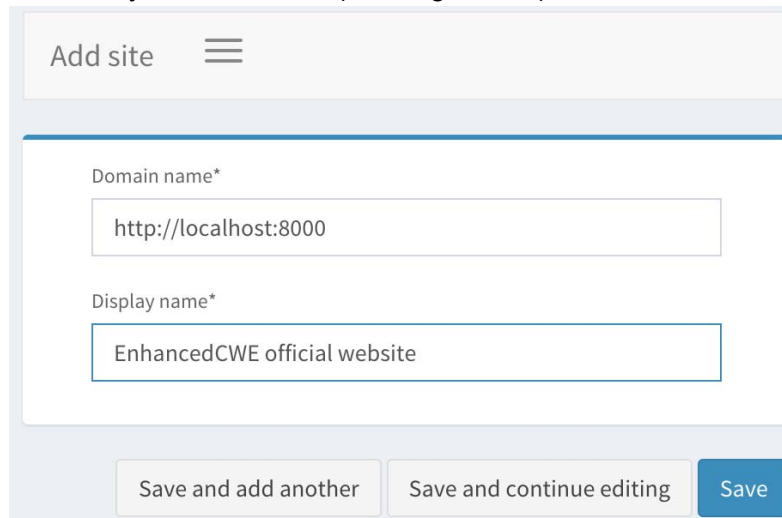
Figure 26: After permission assignment

6. Click “Save” to save the permission assignment.

Site Management

To manage the site information, follow the steps below:

1. In the admin dashboard, navigate to “Sites” -> “Sites”.
2. Click “Add site”.
3. In the “Add site” page,
 - a. In “Domain name”, enter the public domain name of the website.
 - b. In “Display name”, enter a more user-friendly name to make it easier for the users to recognize the website. This name will also be used in the emails that are automatically sent to users. (See Figure 27.)



The screenshot shows a web form titled "Add site" with a hamburger menu icon to its right. The form contains two required text input fields. The first field, labeled "Domain name*", contains the text "http://localhost:8000". The second field, labeled "Display name*", contains the text "EnhancedCWE official website". Below the input fields are three buttons: "Save and add another", "Save and continue editing", and a blue "Save" button.

Figure 27: Add site

4. Click “Save” to save the site information.

NOTE: Please do not add multiple pieces of site information. If multiple sites are added, only the most recently added one will be used.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE June 2016	3. REPORT TYPE AND DATES COVERED Final		
4. TITLE AND SUBTITLE Report Writer and Security Requirements Finder: User and Admin Manuals		5. FUNDING NUMBERS FA8721-05-C-0003		
6. AUTHOR(S) Nancy R. Mead; CMU MSE Studio Team: Sankalp Anand, Anurag Gupta, Swati Priyam, Yaobin Wen, Walid El Baroni				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2016-SR-002		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116		10. SPONSORING/MONITORING AGENCY REPORT NUMBER n/a		
11. SUPPLEMENTARY NOTES				
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS		12B DISTRIBUTION CODE		
13. ABSTRACT (MAXIMUM 200 WORDS) This report presents instructions for using the Malware-driven Overlooked Requirements (MORE) website applications. The site enables requirements engineers and architects to bring the benefit of malware attack analysis to their own product development. They can examine reports of exploited vulnerabilities, frequently augmented by relevant misuse cases, use cases, and overlooked security requirements (MUO) that site contributors have posted. From this data they can search the site to identify security requirements suitable to their own projects. They can also contribute related content and new reports. Users can interact with the site through two applications documented here. The Security Requirement Finder (SERF) allows site contributors to build on malware exploit reports, add MUOs while referencing Common Weakness Enumeration (CWE). The Report Writer application connects to SERF and aids contributors in adding MUOs to the exploit reports. Instructions on performing these activities in both applications are presented here, as well as guides for performing administrative tasks associated with the applications.				
14. SUBJECT TERMS Malware-driven Overlooked Requirements, MORE, Common Weakness Enumeration, CWE		15. NUMBER OF PAGES 95		
16. PRICE CODE				
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102